Opportunity Analysis for Common Access Card Physical Access Control For SSC Norfolk

Version 1.0
10 June 2003

DOCUMENT ACCEPTANCE

PREPARED BY: _____ DATE: 6/19/03
Trevor Bunch, DON eBusiness Operations Office, Commercial Partner

PREPARED BY: _____ DATE: 6/19/03
Larry Gale, SPAWAR Systems Center Charleston, Commercial Partner

ACCEPTED: _____ DATE: 6/24/03
Bonita Armstrong, DON eBusiness Operations Office, Director of Smartcard and CAC Group (Acting)

ACCEPTED: _____ DATE: 6/19/03
Larry Taylor, SPAWAR Systems Center Charleston, Biometrics Project Manager

ACCEPTED: _____ DATE: 6/19/03
CAPT Charles Bell, SPAWAR Systems Center Norfolk, Commanding Officer

RECORD OF CHANGES

The following serves as a history of the change activity affecting this document:

Change Number	Date	Number Of Figure, Table Or Paragraph	A* M D	Title Or Brief Description
Draft 0.0	24 April 2003	ALL	A	First draft
Draft 0.1	09 May 2003	ALL	M	Incorporated 0e4 Comments
Draft 0.2	22 May 2003	ALL	M	Incorporated SSC Charleston Comments
Version 1.0	10 June 2003		M	Incorporated SSC Norfolk Comments

*__A__ - Added __M__ - Modified __D__ - Deleted

Table of Contents

List of Figures

List of Appendices

1. Executive Summary

This report documents the results of an Opportunity Analysis (OA) performed on the Common Access Card Physical Access Control for SPAWAR Systems Center Norfolk (CAC-PAC Norfolk) pilot project by the DON eBusiness Operations Office.

After the CAC was identified as the primary token to be used in physical security, there has been a revolving conversation between the physical security community and the CAC community over how best to meet this objective. The challenge has been to standardize on a specific technology that supports a broad variety of installed electronic security systems, simultaneously enhances the level of security and is scalable to be used throughout DoD. There are a number of technologies to evaluate and the need for operational testing prior to committing to procuring the next-generation of CAC's.

DON eBusiness Operations Office, as the program managers of the DON CAC Program, teamed with SPAWAR Systems Center Charleston and SPAWAR Systems Center Norfolk to test-drive a potential solution. Balancing the existing installed base with a contactless requirement from the physical security community, the team piloted a card configuration with two contactless technologies: HID Proximity for the legacy systems and Mifare to be the new standard. To enhance the level of authentication to enter controlled spaces, fingerprint biometrics were added. To make the system more economical and reduce concerns about biometrics, the biometric templates, a mathematical representation of the fingerprint, were only stored on the Mifare chip. This enabled the existing infrastructure to remain unchanged with the exception of upgrading the readers where the additional security was required.

The pilot was evaluated over a two-month period where user acceptance and system performance was analyzed. Out of the 260 users, only two had difficulty enrolling biometrically and they were able to fully participate in the pilot. Users were generally pleased with the system with some mild concerns about the nature of how their biometric data was being used. Those concerns were resolved by explaining the biometric template resides on a contactless chip on the user's personal identification card and not in a database. Biometric awareness increased by 44% over the evaluation. Users were granted access 97% of the time with two or fewer attempts, aligning with their expectations. The system did experience one major problem with a specific reader, after it was replaced the number of errors or multiple denials returned to acceptable levels. SPAWAR System Center Norfolk management was pleased with backwards compatibility of the solution and how security could be enhanced in a layered approach to meet their requirements. The solution by leveraging the existing infrastructure reduced the cost of the pilot by over 60%. The pilot is still operation and SPAWAR System Center Norfolk is considering using the same approach to enhance security at their warehouses and SIPRNET spaces.

There is an enormous potential to reduce the number of physical security tokens used and move toward interoperability within DoD. This pilot demonstrated that biometrics on a Mifare embedded chip could meet the functional demands of the physical security community for door access control. There are other contactless and biometric technologies maturing that should be evaluated. There are vulnerabilities that need to be investigated. The piloted solution advanced past the current capabilities of the CAC for physical security and is readily available. An action plan is included in this document (**SECTION 6.4**) to assist the DoD Access Card Office in making a decision for the next-generation CAC.

2. Project Description and Background

2.1 Business Problem Satisfied by the Pilot

The DoD Common Access Card (CAC) was developed to address solutions to three business processes and be:

1. The standard identification card for active duty military personnel, Selected Reserve, DoD civilian employees, and eligible contractor personnel,
2. The principal token for logical access to DON computer networks and systems through PKI identity, e-mail, and encryption certificates, and
3. The principal card used to enable physical access to buildings and controlled spaces.

This pilot was designed in Spring 2002 to address concerns with the third business area. To date, the CAC supports multiple technologies for the physical access control community such as bar code, magnetic stripe and integrated smart chip. These technologies have not been adopted by commands currently issued CAC's for a number of reasons. The primary reason is a solution is not easily integrated with their legacy Electronic Security System (ESS). Commands who integrated the CAC into their ESS, for example using the magnetic stripe, quickly discovered that the repeated contact reduces the lifespan of the CAC and their card readers. Considering the cost differential between a CAC ($8.00-$10.00) and a common magnetic stripe card ($0.50), this was a cost deterrent. A third reason for not adopting the CAC into their ESS, was that it did not enhance the security in their access control CONOPS. Bar codes and magnetic stripes are widely used and are becoming easier to duplicate. Solutions with the integrated smart chip, though more secure, were only available if a PIN was used which adversely impacted throughput time. These factors contributed to marginal acceptance.

There exist a number of contactless technologies, which may be incorporated into a standard sized card. The contactless technologies would eliminate the requirement for direct contact between card and reader, thereby reducing the physical wear and tear imposed on the CAC and better accommodating the existing installed base across the DON. It was also decided that the use of biometrics could provide stronger user authentication. Since the CAC contains data storage areas, it is feasible to store a copy of an individual's biometric template for use in subsequent biometric verifications. A number of biometric product vendors have implemented products utilizing contactless card technology for the storage of biometric templates in just this manner. Yet, the number of contactless standards presented another problem in which should be used. The industry leaders included a 125 KHz Proximity standard, and three 13.56 MHz standards. The proximity standard raised concerns about enterprise implementation in regards to a security feature commonly referred to as a facility code. ISO 14443 A and ISO 14443B were mature 13.56 MHz standards, though the short read range (less than 4 inches) could be a limitation in future security applications. ISO 15693 offered a 30 inch read range, but it was a newly adopted standard and was not readily available on the market coupled with biometrics.

2.2 Prior System

SPAWAR Systems Center Norfolk (SSC Norfolk) had recently deployed an ESS consisting of HID Prox Pro card readers integrated with a Lenel Onguard 2002 access control system. All of their employees were enrolled into the Lenel employee database and assigned an access level at the time of their enrollment. After the initial setup, an employee could present the HID prox card to the reader and about a second later be granted entry. A detailed process is detailed below in **Figure 1**.

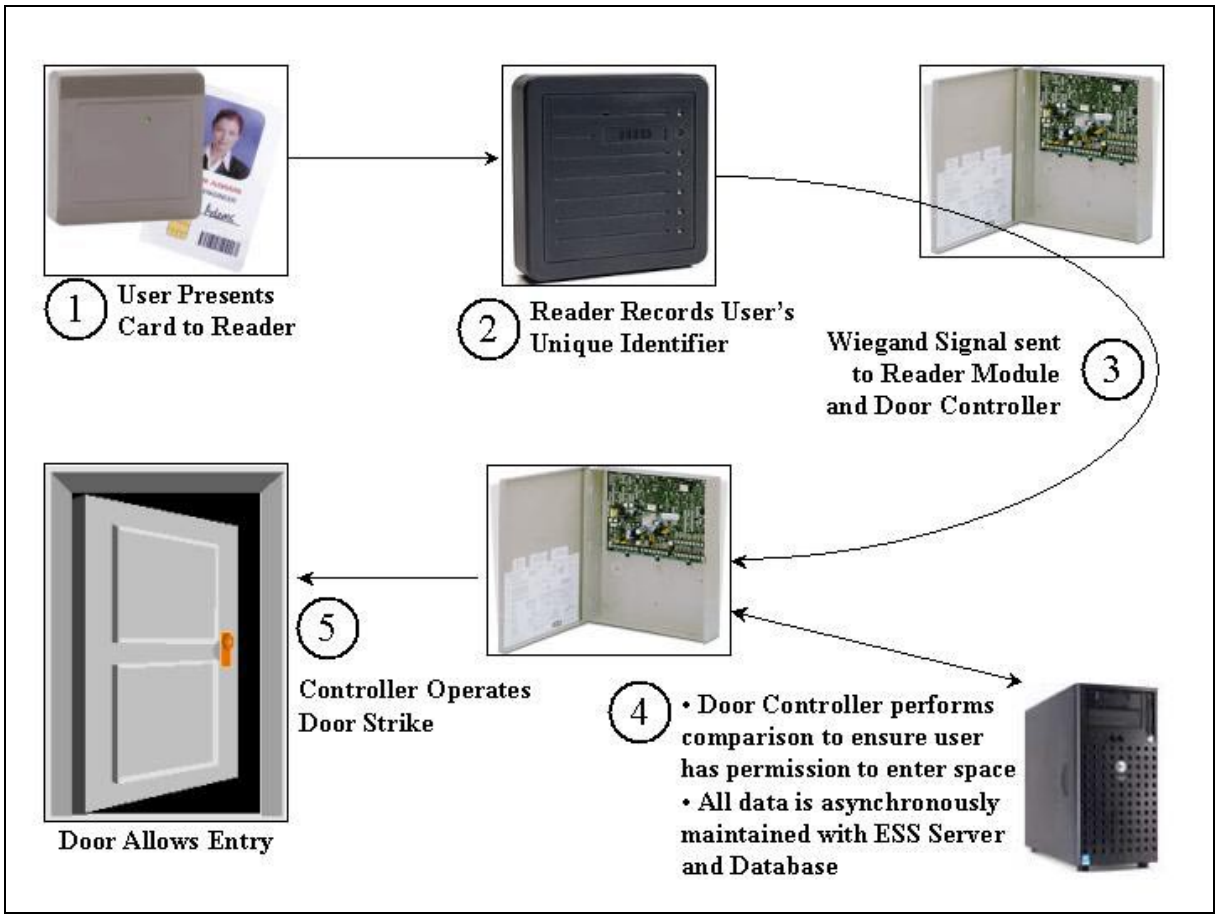

Figure 1: Prior Entry Process

1. The user attempting to gain access to the controlled space holds a proximity card in the vicinity of the proximity card reader.
2. The proximity card reader reads the user's unique identifier (as a Wiegand string) from the proximity card.
3. The reader passes the Wiegand string for that user to the Lenel door controller through the Lenel Reader Module.
4. The door controller compares the access permissions for the user identified by the Wiegand string with the requested door. This data resides on both the controller and the ESS DB and is maintained asynchronously.
5. If the user is allowed access to the requested area, the door controller operates the door strike of the requested door, allowing it to be opened.

2.3 Description of Pilot System

SSC Norfolk was generally satisfied with their system, but acknowledged that anyone holding one of their proximity cards could enter their spaces. For several rooms that contained sensitive computing equipment, management was exploring a means to make the rooms more secure. Having just made an investment into their ESS, it would not be economically feasible to replace that entire infrastructure to enhance three computer rooms (6 doors). The functional requirements for the pilot system was to use the existing infrastructure, add a level of authentication for the three targeted rooms and the solution must remain contactless.

SSC Charleston in conjunction with the DON eBUSOPSOFF CAC / Smart Card Group decided to address the authentication portion with a fingerprint biometric due to its wide availability. Settling on a contactless standard proved more difficult. After collaborating with the DoD Access Card Office (ACO), Smart Card Senior Coordinating Group (SCSCG) and Security Equipment Integration Working Group (SEIWG), it was determined to move forward with a ISO 14443A or Mifare standard. Because the card must work with the new biometric readers as well as the existing HID Prox Pro readers, the team procured cards with both chips embedded. The existing ESS remained largely unchanged, with the exception on integrating the biometric enrollment software.

All employees requiring access to the computer rooms were then issued new badges. Because of the hybrid environment, the system administrator (SA) was required to manually update with a new HID prox card number in the system and write the same number to the fixed identifier portion of the Mifare chip. This was essential for the individual to be recognized as the same person in the Wiegand string sent to the ESS.

After modifying the employee database, the individual's card would be printed and the SA would start the biometric enrollment process. After presenting their index fingers, the system would gauge the quality of the capture. The pilot required at least a medium quality scan on a scale of 5, and a successful test was performed of both fingers before the template was written to the Mifare chip. As means to accommodate different security scenarios, the SA had the ability to control how precise the matching algorithms have to be when comparing a user's fingerprint image to their respective template. Though the pilot used a medium setting as the default, for select individuals who were known to have poor fingerprints, the algorithm setting was lowered to facilitate their entry into spaces.

Below in **Figure 2** and the associated explanatory steps, there is a detailed description of the entry procedure. It should be noted that there are only two differences between the legacy system and the pilot system. Step 2 introduces a new step, where the end user must present their finger for a biometric scan. Step 3 introduces a step where the reader performs a biometric comparison between the live scan and the biometric template on the Mifare chip according to the matching algorithm setting defined by the SA at enrollment. To the legacy ESS system, the introduction of a biometric contactless solution was essentially invisible.

1. The user attempting to gain access to the controlled space holds a contactless smart card in the vicinity of the contactless smart card reader.

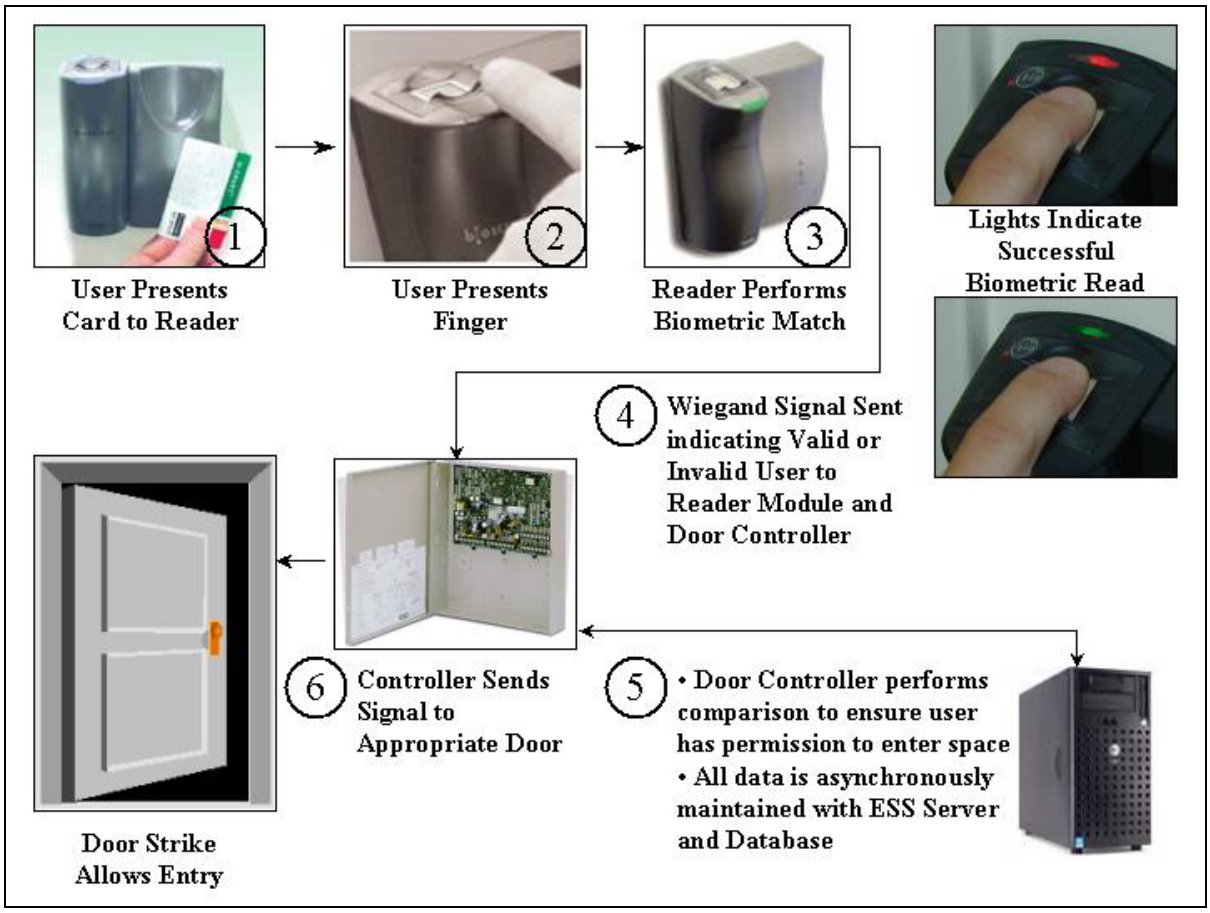

Figure 2: Pilot Entry Process

2. The proximity card reader reads the user's unique identifier (as a Wiegand string) and the user's enrolled biometric template from the contactless smart card. The reader illuminates an orange light, prompting the user to present a finger to the biometric scanner. The user presents the finger, and the biometric scanner acquires a live image of the fingerprint. If the scanner is able to obtain a sufficient quality scan, the light turns green, and the user can remove his finger from the scanner.
3. The reader then compares the live fingerprint with the biometric template retrieved from the contactless smart card. If they match at the predetermined threshold for that user, the user's Wiegand string (unique identifier) is sent to the Lenel ESS. If they do not match at the predetermined threshold for that user, a pre-defined error code stored on the reader indicates an "invalid badge" is sent as a Wiegand string to the Lenel ESS.
4. The reader passes the Wiegand string for that user to the Lenel Door Controller through the Lenel Reader Module.
5. The door controller compares the access permissions for the user identified by the Wiegand string with the requested door. This data resides on both the controller and the ESS DB and is maintained asynchronously.
6. If the user is allowed access to the requested area, the door controller operates the door strike of the requested door, allowing it to be opened. If the user does not have access permission, or the "invalid badge" message was received by the ESS, the door will remain locked.

2.4 Technical Architecture

The pilot leveraged the existing ESS to the greatest extent possible, making only minor adjustments necessary. In **Figure 3**, the pilot system is divided into 4 sections; each will be discussed separately identifying what technical aspects were added to enable the existing ESS with biometrics.

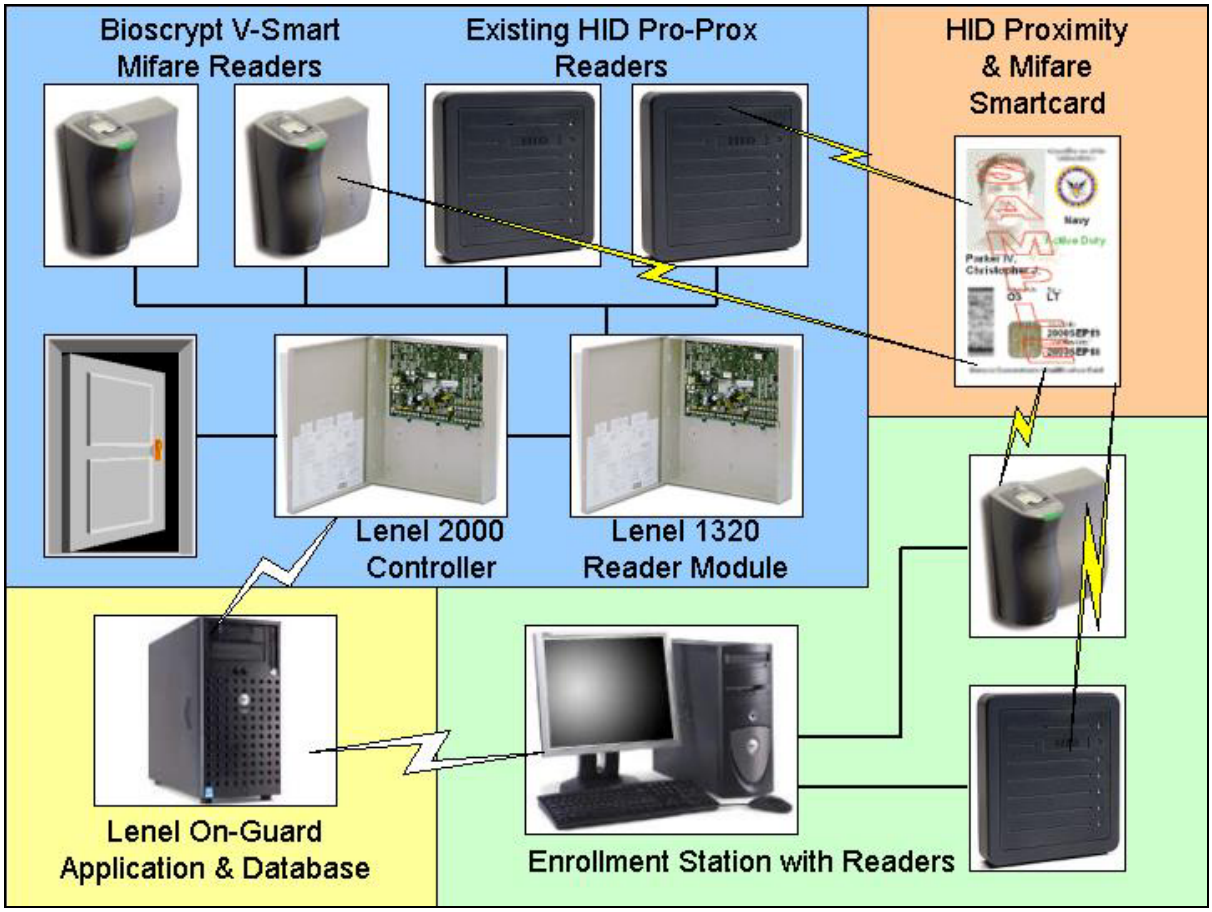

Figure 3: Technical Architecture

2.4.1 Hardware Changes

For the doors where the additional security was deemed necessary, the HID ProxPro 5355 readers were replaced with Bioscrypt V-Smart readers. The Bioscrypt readers did require more current than the existing Prox readers, therefore, additional power supplies were installed. The remaining Prox readers continued to draw their power from the Lenel panel. Door 5 did not have any hardware installed prior to the pilot: to equip it for the pilot, the team installed a Door Strike, Balanced Magnetic Switch (BMS), Request to Exit / Passive Infrared Detector (REX/PIR) and the Bioscrypt V-Smart Reader.

2.4.2 Card Architecture

To ensure that the card worked on both the existing readers and the biometric readers, the team procured a HID Proximity and Mifare Card (1431) that incorporates two antennae. One is used for communicating with a 125 kHz Proximity reader, and the other communicates with a 13.56 MHz Mifare contactless smart chip reader. (See **Figure 4**) The Mifare Chip has 1Kb of space to store data, specifically biometric data. By utilizing this design, the team did not have to secure a database where everyone's templates were stored and the users reacted more positively to the pilot.

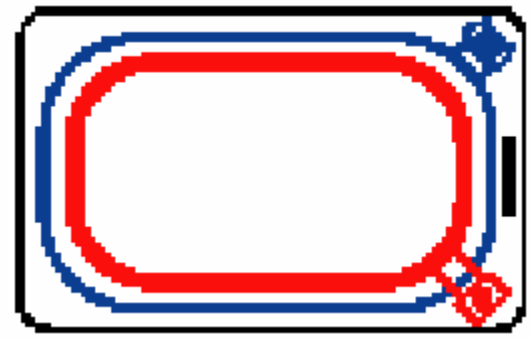

Figure 4: Dual Antennae Layout

The Mifare chip has 16 sectors numbered 0-15 and 4 blocks per sector numbered 0-3. (See **Figure 5**) The fourth block in every sector is unavailable for use by Bioscrypt. Two finger templates were stored on each card, and each template required 352 bytes of storage (the templates are actually 348 bytes in size). These are indicated as blue for the primary template and magenta for the secondary template in **Figure 5.**

The black blocks are used by the manufacturer and were unavailable to be written to for customized uses. The dark green block (Sector0-Block1) is the layout block and it is used by Bioscrypt to specify layout of data on card such as where the templates are located. The red block (Sector8-Block1) is the administration table: it serves as a pointer to the Layout bock for the Bioscrypt Mifare reader. The green block (Sector0-Block2) stores user data, at this time only the User ID. The V-Smart reader uses it to determine if the user has access to the space. When a biometric access grant or deny occurs the reader sends a Wiegand string to the Lenel 1320 panel. For SSC Norfolk, the Wiegand string for a match contained the Facility Code stored on the reader and the User ID stored on the 14443 chip. For mismatches a configured Wiegand stored on the reader was sent to the Lenel 1320 panel. The results were logged into the Lenel OnGuard Database. To make the new system backward compatible the Facility Code was placed onto each of the new readers card to match the existing HID Facility Code previously written on to the cardstock.

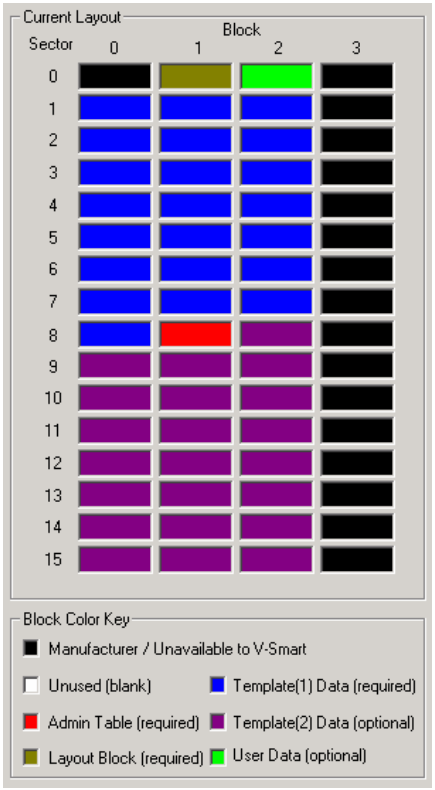

Figure 5: Mifare Chip Data Map

2.4.3 Enrollment Integration

Participants were enrolled into the ESS using the Lenel OnGuard badging system workstation. The badging system was hosted on a PC, running the Microsoft Windows 2000 Professional operating system, and containing 256 MB of RAM and 20 GB of disk storage. The badging software was part of the existing Lenel OnGuard system and the cards printed for the pilot conformed to the current SPAWAR ID Configuration.

During enrollment via the Lenel badging workstation, the 26 bit Wiegand string comprising of the facility code and card number, was imported and assigned to personnel in the existing Lenel ESS database. This value is reported to the ESS when used at the existing proximity readers, which compares the user's permissions with the access requested at the reader's location. If the user is authorized, the backend sends a command to the door strike, allowing the door to be opened

For biometric enrollment, the card was then taken to the biometric enrollment station. For the pilot, the same PC used for Lenel Badging had Bioscrypt VeriAdmin software (version 4.30) installed and a Bioscrypt V-Smart reader attached to the serial port of the enrollment station. The user would have two fingerprint templates taken and stored to the card with their user profile as shown in the **Figure 5**. Once the user is enrolled biometrically, the card can be used at either the existing proximity readers, or the biometric readers. When the user presents the card to a biometric reader, the templates are retrieved from the card, and a comparison is performed against a live scan from the user. The comparison threshold is set in two locations, one is specified for each V-Smart unit (used to heighten the matching requirements for more secure locations) and the other is defined at enrollment and stored on the Mifare chip (used to customize matching requirements for persons with poor biometric samples). Upon a match, the Wiegand data string associated with that user's profile is retrieved and transmitted to the ESS backend system, which compares the user's permissions with the access requested at the reader's location. If the user is authorized, the backend sends a command to the door strike, allowing the door to be opened.

2.4.4 Backend Application & Database

The backend ESS system does not distinguish between the ProxPro readers or the Biometric readers, because both send the same formatted Wiegand signal. There were no changes made to the ESS to biometrically enable the system: no additional modules or data fields were required. The workstation configuration used at Norfolk can be found in the table below:

System Requirements	
Application	Lenel On-Guard Access Version 5.9
Operating System	Windows 2000
Memory Required	256 MB
Database	SQL Server 2000

Figure 6: ESS System Requirements

3. Project Goals, Objectives and Metrics

3.1 Project Goals and Objectives

3.1.1 Immediate Access Control Improvement

The immediate objective of this biometric pilot was to determine the benefits of integrating contactless biometric technologies into the existing ESS to protect secure areas. The contactless technology evaluated in the pilot complied with International Standards Organization (ISO) standard 14443 Type "A", also known as Mifare technology. The pilot also evaluated placing a biometric fingerprint template on the contactless smartcard and allowing the biometric reader (specifically, the Bioscrypt V-Smart) to perform the match comparison. It was designed specifically to determine if it was operationally feasible for the biometric template to be in possession of the biometric owner and eliminate the need to store a biometric database in the ESS. It also addresses the biometric owner's concerns about how their personal information is being used and stored.

3.1.2 Next-Generation CAC

Beyond the immediate goal of improving access control, the larger objective is to provide operational data on contactless technology for consideration to be placed on the next generation of Common Access Cards.

3.2 Project Metrics

Three categories were devised to measure the success of the pilot in attaining the goals mentioned above. The majority of the metrics deal with intangibles, such as user's response to the using biometrics and how it enhanced security. By leveraging the existing infrastructure, some potential financial benefits can be realized, making a layered security approach economically feasible for cash-hungry commands: this is dealt with in more detail in **Section 4.3**.

3.2.1 User Acceptance

The metrics for user acceptance were designed to measure overall satisfaction from end-users: ease of use in the operational environment; an increased knowledge of biometrics; and any increased feeling of security among users of the system. These metrics were captured using pre-pilot and post-pilot survey forms that were completed by users of the system, as well as through anecdotal reports from users and management and problem reporting forms filled out during the course of the pilot. Striking the right balance between level of security and inconvenience to the end user is a fine line that the pilot hoped to find through education. Goals for user acceptance were established with the perception that users would generally respond negatively to the system. For general user acceptance, the team set an ambitious goal that the majority of users would approve of the pilot and respond positively to questions of ease of use. Recognizing the common user reaction to the use of biometrics as an invasion of privacy, the team set modest goals of a positive response for those metrics and also compared those results to the education process used in the pilot.

3.2.2 System Performance

The metrics for system performance were designed to provide an assessment of how well the system performed during the pilot with respect to accuracy, error rates in an operational setting, accuracy and speed of enrollment, and ease of administration of the system. These metrics were based primarily upon detailed review of all system logs, along with surveys of administrators of the system and other anecdotal reports. Goals for these specific metrics were set arbitrarily. The reduction in error rate was set at 50% reduction in the first month and an additional 25% reduction in the second month. The team also set a goal that persons would be granted access on their first attempt 90% of the time. The other metrics in this area were gathered through observations with no target in mind.

3.2.3 Enhanced Security

The metrics for enhanced security are a measurement of assurance that the individual attempting to use a card (token) for access is in fact the authorized owner of that card. These metrics were based primarily upon qualitative statements provided by managers and administrators of the system. The obvious goal was for the on-site security managers to endorse the pilot as an asset in fulfilling their mission.

3.3 Alignment of Pilot and Enterprise Goals

The goal alignment table in **Figure 7** demonstrates how the enhanced capabilities offered by the CAC-PAC Norfolk system directly contribute to the satisfaction of enterprise goals and objectives.

Enterprise Goals & Objectives	Pilot-Enabled Capability	Key Performance Indicators
Use the CAC as the Physical Access Token	Contactless Technology	Evaluate 14443 A for inclusion on future CAC's
		Explore means to standardize how the contactless chip can be used across the enterprise.
Enhance Physical Access Control	Biometric Technology	Increased Biometric Awareness
		Increase User's feeling of security
		Provide User Authentication
Determine Cost and Time Effective Means to Enhance Security	Leverage Existing ESS	Minimize upgrade costs to backend systems
	Increase Security only where Required	Only upgrade where there is a security requirement, as opposed to reacting to technology constraints.

Figure 7: Goal Alignment Table

4. Analysis of Pilot Results

4.1 Evaluation of Metrics

This section presents an assessment of the quantitative success rates achieved in attaining the previously established goals of the project. A detailed description of each metric, the goal for which that metric is applicable, and the results obtained through quantitative analysis are provided. The metrics were obtained primarily from two sources: user responses to pre-pilot and post-pilot surveys and error logs in the ESS. The system administrators and design engineers contributed to the qualitative and financial benefits of the pilot.

4.1.1 User Acceptance

As stated in **Section 3.2.1**, by adding an additional step in the entry process and knowing concerns that individuals have about their biometrics captured, the team expected end-users to respond negatively to the pilot. However, the team expected to balance the negative feelings with an increased sense of security and awareness of biometrics. User acceptance was measured using five different metrics: (1) overall satisfaction, (2) ease of access to controlled spaces by authorized users, (3) increased familiarity with biometrics, (4) increased feeling of security in user spaces, and (5) perception of invasiveness of the technology.

The results were surprising. Although there were several comments regarding inconveniences of placing the finger on the reader where the user was carrying items or experienced a longer wait time for the door to open (3-4 seconds with the biometric compared to 1-2 seconds without the biometric), 61% of users approved of the pilot and only 19% expressed a disapproving sentiment. The ease of use question revealed that under pre-pilot conditions 83% experienced no problems and there were no instances where it interfered with their work. Under pilot conditions, the average user experienced minor problems and 5 users reported that the problems seriously interfered with their work. This reveals that users found gaining access to their workspaces more difficult using the biometric technology than their previous HID system. While this was an expected result, the ongoing problems at Door 5 (see **Section 5.1**) may have negatively impacted this rating. There were also several comments on the post-survey that indicated that the solution is time consuming and should not be used in high traffic control points. Surprisingly, the decreased ease of use did not negatively affect their satisfaction with the pilot.

The pilot team expected with the education process conducted prior to enrollment to increase biometric awareness and reduce privacy concerns, resulting in an increased sense of security that would offset the concerns. The education process worked to a certain degree. The majority of users were not familiar with biometrics at the beginning of the pilot and towards the end the average user was in a neutral stance. Though the pilot exceeded goals by increasing biometric awareness by 42% and the percent of those familiar doubled, it still should be noted that only 22% expressed familiarity. This may in part explain why there was no significant change in the users' perception that security had been increased (for the security administration opinion see **Section 4.1.3**). Another and perhaps more probable reason is that the users already felt secure in their spaces. The users' comments did not indicate the reasoning. Our final educational

metric dealt with the perception that biometrics was an invasion of their privacy. There was a 12% decrease in the user perception that biometrics are invasive: the average user is between "Not Invasive" and "Somewhat Not Invasive". Surprisingly, users' opinion regarding the invasiveness of biometrics did not correlate to their opinion regarding enhancing security offsets privacy concerns: they moved slightly towards disagreeing from a neutral stance. These results should be taken in the light that 22% of users expressed familiarity with biometrics. User comments indicate that there remained some questions regarding the use of the biometric data: "I would like to know more about the extent my bio data will be used. That would raise my comfort level with the product and its intended use." As documented in the lessons learned, the results will impact how user orientation (**Section 5.3**) is handled in the future.

Overall, the users' acceptance of the pilot exceeded expectations. The most frequent complaints were the time it took to gain access and number of attempts, which will be explored in the next section. Those can be mitigated through additional training and increasing the quality of the template at enrollment. Better monitoring during the pilot would have identified and addressed those issues. There was no direct opposition to using a biometric to gain access, but survey results suggest that there is room for improvement in the education process. A 61% approval rating far exceeded expectations.

For detailed survey results, please see **Appendix A: Detailed Users Survey Results**.

4.1.2 System Performance

This metric provides an assessment of the actual performance of the pilot system during the test period. It is based primarily upon the logs from the ESS, along with surveys of administrators. The specific metrics for system performance include: (1) Percent First Attempt Access Granted, (2) Decrease in errors, (3) Enrollment Throughput, and (4) Ease of Administration.

In order to determine the convenience of the system for the end-users, the number of attempts before successful entry was measured. The target for the pilot system was for 90% of users to gain access on their first attempt. Excluding the ongoing problems at Door 5 (see **Section 5.1**), the user was granted access on the first attempt 89% of the time and granted access with 2 or fewer attempts 97% of the time. This aligned well with end-user's expectations.

As the education and familiarity increased using the biometric readers, it was expected that the access attempt failures would decrease over time. During the first week of the pilot, over 17% of attempts did not result in access grants. By the end of September, the error rate dropped 26% to 12.5% and an additional 8% by the end of the evaluation in October. The goal for this metric was 50% reduction for the first month and an additional 25% reduction the second month. The goal was not met, but given the 97% success rate above and the failure figures includes abandoned attempts, invalid badges and other log messages that did not result in access granted: the team was pleased with the results.

Another measure of convenience that was measured during the pilot was the enrollment process. Each participant was required to enroll two fingerprints prior to using the

system. Enrollment occurred during business hours and took the employee away from their work and every effort was made to make sure that they were properly educated and enrolled during this time. The average enrollment took less than 2 minutes with two attempts. Several users were enrolled in less than 60 seconds on their first attempt. There were two individuals who had unusual difficulty enrolling. One individual was a burn victim as a child and it reduced the quality of the fingerprint. Another user had such poor quality fingerprints that the enroller modified the verification thresholds for the individual. This solution was only used once and when all other methods failed, and only because the system allowed customization on a per-user basis.

Ease of administration is largely a subjective measure, though there is a perception that when biometrics are included the complexity increases exponentially. The two administrators for the system did not have any problems either participating in the pilot or administrating it. They described the enrollment process as “Easy” and credited the system for increasing the level of security in the facility. The introduction of biometrics did not impact the ability to administer the system.

For detailed analysis, please see **Appendix B: System Statistics**.

4.1.3 Enhanced Security

The metrics for enhanced security provide an increased assurance that the individual attempting to use a card (token) for access is in fact the authorized owner of that card. The pilot was not intended to record the accuracy of the biometric devices in regards to False Acceptance Rates (FAR) and False Rejection Rates (FRR), rather measure the reactions of users and how it functioned in an operational environment. User perceptions of security have already been discussed, in **Section 4.1.1** above. However, it is important to assess the perception of security among the managers and administrators, as well as among the general user population. These metrics were based primarily upon qualitative statements provided by managers and administrators of the system.

SSC Norfolk designated two administrators, thus making quantifiable analysis based on administrative surveys not statistically significant, but valuable due to their first hand experience of the system. Their reported feelings of security in the spaces both went up as a result of the pilot. Their responses to the question “How secure do you feel in your spaces?” increased one level, from a mean of 3.5 (slightly secure) to 4.5 (secure to extremely secure).

Managers reported that their goal of gaining better control of computer room access was achieved, and that the system helped limit access to the computer rooms to 260 authorized users. In addition, they plan to continue to use the system after completion of the pilot, and would like to add contactless biometrics to additional areas in the future. This seems to indicate a strong feeling among managers and administrators that the biometric solution did, in fact, offer enhanced security for controlling access to secure spaces.

4.2 Qualitative Analysis and Intangible Benefits

In addition to the metrics described above, the Norfolk Biometrics Pilot produces several less quantifiable, yet significant benefits for both the customer and the enterprise. These include:

Integration of biometrics with existing ESS – The pilot demonstrated the ability to integrate a biometric authentication solution utilizing contactless technology into an existing enterprise legacy ESS. No large-scale replacement of legacy security infrastructure is required, which could lead to significant savings in future deployments. While this assertion cannot be made for all ESS's, the design laid out in this pilot makes it a promising prospect that would avoid additional cost associated with a full scale upgrade.

Minimize Privacy Concerns – Through the education process, participants were made aware that their biometric templates were stored on their card rather than in a database. They were also instructed that the information on their card was a biometric template or a mathematical representation of their fingerprint, and it could not be reverse engineered to reconstruct their biometric information. These two design considerations alleviated most concerns about using biometric technology.

Validation of Security Access – By upgrading the three rooms to a biometric entry, management was able to review who was allowed access to those spaces when everyone was requested to enroll their biometric. Even though this audit procedure is already accounted for in SSC Norfolk's CONOPS, the pilot identified areas where access could be restricted further. For example: concerns about the air conditioning created a situation where several individuals would have to access the room to check the status. If a person was unable to perform this duty, an alternate used their Prox card to check the air conditioning. There was no assurance that who actually entered the room was the person identified on the card, and an equal concern to hand out Prox cards to the entire air conditioning maintenance crew. The audit performed prior to biometrically enrolling persons allowed the security managers to revalidate who had access to the spaces and assured them of who was entering the spaces.

Scaled Upgrades – Management at SSC Norfolk was impressed on how a portion of the ESS could be upgraded to biometrics based on their security requirements. They plan to continue use of the pilot system, and see the value to add biometric authentication for other locations, such as warehouse areas and SIPRNET rooms. As their security requirements change, there is a means to adjust areas of the ESS without a significant investment in technology or administrative resources.

4.3 Financial Analysis

Unlike a typical Cost Analysis where productivity gains are measured, increasing the level of security is more difficult to quantify. For the financial analysis of this pilot, we will focus on how the pilot explored alternatives to limit the financial resources required to upgrade to biometrics. The design objectives were that the biometric must reside on a contactless portion of the card and that as much as possible of the existing ESS should be leveraged. Within these design constraints, two different scenarios were created that a command could face:

1. The immediate need to upgrade a subset of their spaces and maintain existing system.
2. The need to overhaul their entire security system and determine if biometrics should be included.

Alternative approaches for each scenario will be explored and their financial resource requirements will be defined.

4.3.1 SCENARIO 1: Sector Upgrade

In this scenario, there is requirement to increase the level of user authentication for a specific area or sector. There are three approaches that one could take: integrate biometric readers into the existing ESS, build the sector ESS from scratch and build the sector ESS from scratch then integrate it with the existing ESS. Integration with the existing ESS carries the benefit of consolidated administration, but there are risks in the areas of backwards compatibility and adding complexity to the card stock. Building a sector ESS avoids the backwards compatibility risks, but places additional strains on administration, maintaining the system and could potentially require users to carry multiple cards. The third approach of integrating the two systems at the end presents an additional cost above the second approach that would price itself out of consideration, thus it was not pursued any further.

In **Figure 8**, the sector upgrade costs are placed along side the stand-alone sector installation. The sector installation does not require HID Proximity Chip embedded in the card for backwards compatibility, thus would save approximately $3 per card. This was the only advantage the sector installation had over the sector upgrade. For the size of pilot in SSC Norfolk, the stand-alone sector installation would cost approximately 167% more than the upgrade, not align with enterprise goals and still carry all of the disadvantages mentioned above. The sector upgrade piloted at SSC Norfolk could be applied to any ESS that accepts Wiegand formatted strings. It should be noted that the actual pilot costs were larger than the typical sector upgrade due to having to completely install a new door and the resources it took to evaluate the pilot for two months.

Description		Actual Pilot Cost		Sector Upgrade		Sector Installation	
Cost of Pilot System	Unit Cost	Quantity	Extended Costs	Quantity	Extended Costs	Quantity	Extended Costs
Equipment							
Bioscrypt Reader	$1,000	8	$8,000	8	$8,000	8	$8,000
Power Supplies	$148	5	$740	5	$740	5	$740
Door Strike	$250	1	$250	0	$0	6	$1,500
Cards	$8 / $5	500	$4,000	500	$4,000	500	$2,500
Printer	$500	0	$0	0	$0	1	$500
LNL-2000 Intelligent System Controller	$1,069	0	$0	0	$0	1	$1,069
LNL-1320 Card Reader Module	$538	0	$0	0	$0	3	$1,614
Miscellaneous Material	$500	1	$500	0	$0	4	$2,000
Subtotal Hardware			*$13,490*		*$12,740*		*$17,923*
Software							
Lenel 32 Onguard	$9,000	0	$0	0	$0	1	$9,000
Bioscrypt VeriAdmin	$0	0	$0	0	$0	0	$0
Subtotal Software			*$0*		*$0*		*$9,000*
Total Equipment & Software			*$13,490*		*$12,740*		*$26,923*
General & Administration Fees	*10%*		*$1,349*		*$1,274*		*$2,692*
Labor + Travel + Per Deim							
Design Services	$1,000	14	$14,000	6	$6,000	20	$20,000
Installation	$1,000	34.3	$34,300	28	$28,000	70	$70,000
Training	$1,000	5	$5,000	5	$5,000	7	$7,000
Evaluation	$1,000	30	$30,000	0	$0	0	$0
Subtotal Labor			*$83,300*		*$39,000*		*$97,000*
Subtotal Non-Recurring Costs			***$98,139***		***$53,014***		***$126,615***
Recurring System Life Cycle Maintenance, Operations & Support (Projected)			$0		$0		$15,000
Total Annual Pilot System Costs			**$98,139**		**$53,014**		**$141,615**

Figure 8: Sector Upgrade Financial Comparison

4.3.2 SCENARIO 2: Overhaul Costs

For this scenario, it was assumed that a command would be installing or replacing readers on 100 doors and would require an initial purchase of 1000 cards. Two objectives were compared: contactless entry and biometric entry through contactless technology. Contact and biometric-only solutions did not meet the design objectives of this pilot and are considered out of scope for comparison purposes. Available technologies were compared within objective areas. Of the hundred new readers, only 25% would require biometric authentication due to a layered security design. Though the labor for design and installation cost may vary for each; the cost differential was determined not to be significant and would not affect the technology decision.

In **Figure 9**, Four potential solutions are offered for comparison. The prox contactless solution is the simplest, inexpensive and most commonly deployed solution in the DON. If the sole objective was for the access control system to be contactless, then it proves to be a better choice over the Mifare contactless that costs 13% more. There are disadvantages to the Prox solution when considering interoperability as discussed in **Section 2.1** and the chip is read-only. Therefore the most cost-effective means to upgrade to biometrics would be under the model used in this pilot (Dual Chip Antennae) or convert the whole system to Mifare.

Deciding on the contactless biometric solution, existing infrastructure and card/reader ratio are the major drivers. The pilot demonstrated that utilizing the existing infrastructure could dramatically reduce the cost. This may be relevant if the command wants to leverage their existing Prox readers. Another consideration is that the Prox readers are significantly less costly than the Mifare readers. Even with the Prox/Mifare cards being more expensive, there is a substantial larger investment being placed in readers making the Prox/Mifare solution preferable. On the other hand, a pure Mifare solution would only cost 5% more and would reduce recurring card costs.

Description	Unit Costs	Contacless Only		Contactless and Biometrics	
		Prox	MIFARE	Prox/MIFARE	MIFARE
Card Stock	1000 Total				
Prox	$3.65	$3,650.00			
MIFARE	$5.00		$5,000.00		$5,000.00
Prox/MIFARE	$8.00			$8,000.00	
Subtotal Card Stock		*$3,650.00*	*$5,000.00*	*$8,000.00*	*$5,000.00*
Readers	100 Total				
Proximity Reader	$350.00	$35,000.00		$26,250.00	
MIFARE Reader	$500.00		$50,000.00		$37,500.00
MIFARE Biometric Reader	$1,000.00			$25,000.00	$25,000.00
Subtotal Readers		*$35,000.00*	*$50,000.00*	*$51,250.00*	*$62,500.00*
Misc. Hardware					
Power Supply	$148.00			$3,700.00	$3,700.00
Subtotal Misc. Hardware		*$0.00*	*$0.00*	*$3,700.00*	*$3,700.00*
Software					
Bioscrypt VeriAdmin				$0.00	$0.00
Subtotal Software		*$0.00*	*$0.00*	*$0.00*	*$0.00*
General & Admistration Fees		$5,140.45	$7,315.00	$8,372.35	$9,469.60
Labor for Design and Installation		$100,000.00	$100,000.00	$100,000.00	$100,000.00
Subtotal Non-Recurring Costs		***$143,790.45***	***$162,315.00***	***$171,322.35***	***$180,669.60***
Annual Life Cycle Support (Projected)		$1,000.00	$1,000.00	$1,000.00	$1,000.00
Total Annual Pilot System Costs		**$144,790.45**	**$163,315.00**	**$172,322.35**	**$181,669.60**

Figure 9: Installation Cost Alternatives

5. Pilot Lessons Learned

The lessons learned from this pilot were derived from the comments and responses provided by users of the system on the post-pilot survey forms, comments from administrators of the system, and written and oral communications from the SSC Norfolk management.

5.1 Active Monitoring

During the course of the pilot, one of the doors used for biometric access experienced an excessively high failure rate, as defined as requiring more than two attempts to gain access. These failure rates showed a clear downward progression over time at Door 5. Eventually, the biometric reader installed at that door was replaced during week 7, on the assumption that the unit in question was faulty. Prior to that replacement, some users would make multiple attempts (8 or 9 attempts) before gaining access to the controlled space. These failures went undiagnosed for longer than they should have, as is illustrated by the following graph, which shows the percentage of users gaining access through a door on their first attempt during the 9 weeks of the pilot. Note that the zero error rates for Door 5 on weeks 3 and 5 corresponded to an extremely low rate of usage for that door during those weeks. After the biometric reader was replaced in week 7, the rate dropped to a level more in line with that seen on all of the other doors. Failure to recognize the problems with this unit caused considerable negative opinion among users who were denied access at that location.

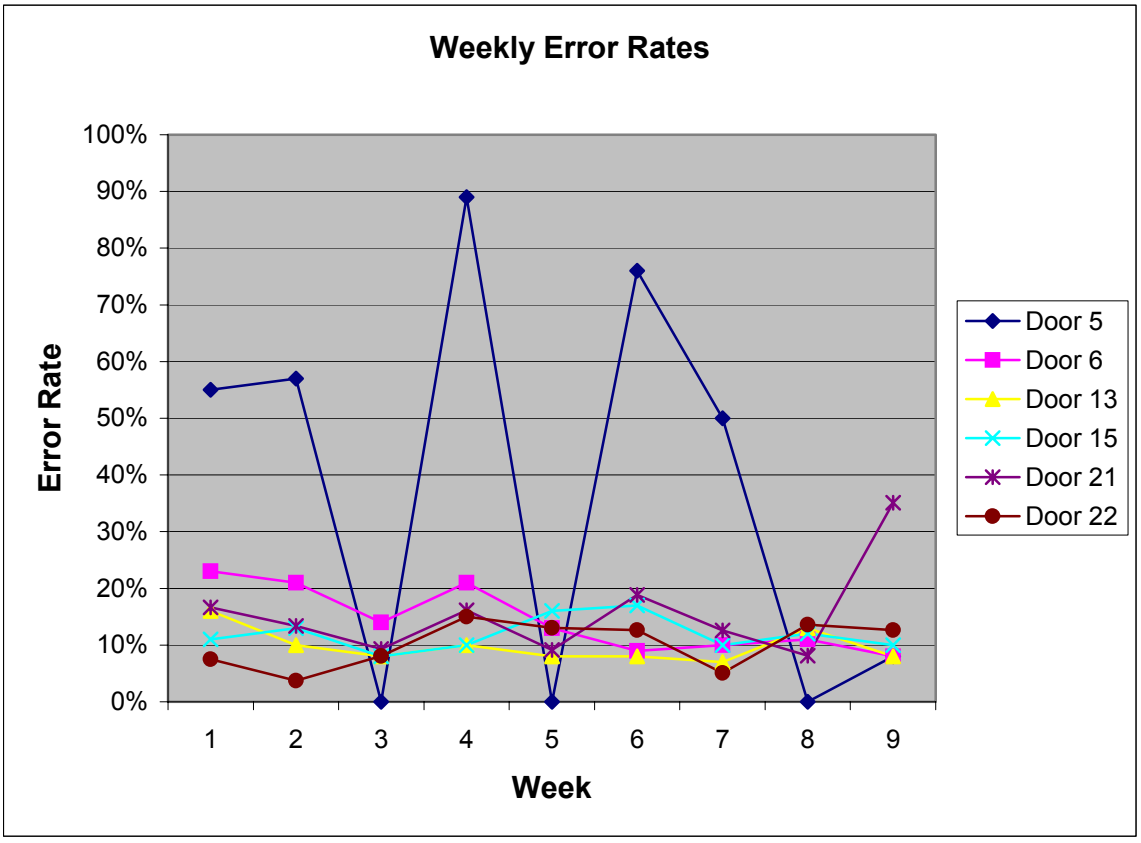

Figure 10: Door Error Rates by Week

LESSON: *All system activity, including ESS logs and user reports of problems, should be monitored regularly and frequently by a knowledgeable administrator to allow the rapid identification of problems in any of the system components, including hardware, software, or configuration of the system.*

5.2 Streamline User Feedback & Response

Closely associated with the lesson learned in **Section 5.1**, the method in which users provide feedback with system administrators must be forwarded to the appropriate personnel and the user should receive acknowledgement and resolution in a timely manner. This is illustrated by another problem experienced at Door 5. After the new reader was installed, it was not correctly configured for access into the ESS. This led to a scenario in which several users were biometrically verified, but were denied access by the ESS. The users could not determine why they were not permitted access and reported it as the same error previously experienced. The ESS logs revealed that only two errors for Door 5, were being issued: "Invalid Badge" meaning the live biometric did not match the template and "Invalid Access Level" meaning the user was not permitted access in the ESS. Given that the green indicator on the biometric reader signified that the user has been biometrically verified and the system administrator was previously allowed entry, the problem was correctly identified.

The breakdown in communication between the end users and the system administrators spurred negative feedback about the biometric security system. The level of support provided to the users participating in the pilot was not sufficient to allow for the immediate and timely resolution of problems they experienced. This was highlighted in the qualitative summary provided by IT management at the conclusion of the pilot, when they identified a clear need for more direct contact with users having problems. While paper forms (exemption reports) were located at doors for users to report problems, the number of entries made by users is significantly less than the number of problems observed in the ESS logs. This is most likely attributed to two reasons. Users generally did not perceive any response to the problems that they did report, and users did not see the benefit of reporting the same problem multiple times. So they simply stopped actively reporting their experiences.

LESSON: *Users must be provided with a way to provide feedback to administrators and project personnel on any problems they experience, and their feedback must be acknowledged and acted upon in a timely manner. Failure in this area increases user frustration, which will inevitably skew their opinions of this technology in a negative manner.*

5.3 User Orientation

Users experienced occasional problems because they treated the contactless card like their traditional proximity card, or did not correctly place their finger on the biometric device. These problems were evident in the user's comments. For example, one user reported that he "had to swipe badge 3 to 4 times to get yellow light for finger print". This shows that the user in question wasn't adequately briefed on the differences between traditional prox cards and the contactless smart cards used in this pilot. A "swipe" is usually sufficient for reading prox cards, which have a longer read range and transfer a smaller amount of data. However, the contactless smart cards must be held very close to the reader, and must be held there for a long enough time to allow the biometric template to be read. Failure to hold the card close enough, or for a long enough time, will lead to card read errors.

Other users correctly diagnosed their own problems in regards to finger position. One user commented, " Averaged 1 failed attempt to get in out of approx. every 10 attempts. Normal problem was that it did not accept my fingerprint when I placed it on the reader. Seems related to position of finger on reader." Another user came to a similar conclusion that "Perhaps familiarity with the device with continued use would help." Regardless of the user's awareness of the problems they experienced, this confusion could have been eliminated by providing better training and explanation of the technology in any training sessions, and during the enrollment of users.

***Lesson**: It is important to provide quality training and orientation of users participating in a pilot project, especially one using multiple technologies (such as contactless smart cards and biometrics) where the users have limited experience.*

5.4 Support from Multiple Vendors

During pilot implementation, the Bioscrypt readers were programmed to send a Wiegand string identifying a user when the cardholder's identity was biometrically verified. This information was logged in the Lenel ESS logs. However, when a user failed to verify biometrically, a predefined Wiegand string equating to a non-existent user, was sent to the Lenel ESS logs. Unfortunately, this did not allow the system administrators to determine which users were failing to verify biometrically. Only through contextual examination of the logs was the System Administrator able to make an educated guess regarding who had experience problems.

For example, if a log entry showed that a user was granted access, but that access was preceded by one or more failed access attempts in close temporal proximity, then those failures were assumed to be failures by the individual who was eventually granted access. When the time differentials were on the order of 30 seconds or less between failure and acceptance, this is probably a reasonable assumption. A better solution would be the Bioscrypt reader providing the identity of the user who failed to authenticate biometrically. After the pilot was completed, research with technical personnel at Lenel and Bioscrypt revealed that a method exists which could be used in future implementations. This method involves programming the Bioscrypt reader to send the user information with reversed parity when a user fails to verify biometrically. The Lenel system must be configured to interpret that parity reversal in the desired manner. If this information had been available prior to the pilot implementation, the systems administrators would have been better able to identify individuals who were experiencing problems during the pilot. This would have likely led to improved performance of those users, and ultimately, to a higher level of acceptance of the technologies tested during the pilot.

***LESSON:** In order to successfully integrate biometric systems, which utilize products and technologies from multiple vendors, it is important to identify key personnel from each vendor to rapidly resolve technical problems and issues identified during the course of pilot implementation. They would also benefit from learning of new requirements and participating in the evaluation criteria of their products.*

5.5 Align Data Collection with User Expectations

The pilot project is primaryly a technology proof of concept and the entire management of the project revolved around that particular aspect. Our test plan exhaustively tested each component of the system, which left little focus on how to effectively measure user acceptance.

Our pre and post-surveys were developed to gauge the users' thoughts regarding the use of biometrics in their workspace, privacy concerns and the efficiencies of the access control system. More attention should have been given to the culture of the users. Pre-Surveys were paper-based and the Post-Surveys were a distributed MS Word document. Most of the pilot users were IT professionals and they found the format inconvenient and at times confusing. There were several comments clearly that took issue with the survey itself: "Design future survey forms so they can be properly filled out online." In the end, an online survey would have benefited the team as well in collating the results.

LESSON: *Data Collection should be customized to meet the users' expectations and skill sets. When developing user surveys, it should be clear to the target audience what you are speaking about, providing definitions when necessary and in a format that is consistent with the environment that they consistently work in.*

5.6 Enrollment Logs

An additional process that would benefit the system would include the collection, during enrollment, of enrollment quality statistics (i.e., the quality of fingerprint obtained during enrollment). Storage of such data would facilitate the identification by administrators of those users who may require a biometric re-enrollment. Either a better quality enrollment of the same finger, or a selection of another finger for enrollment could be dictated based upon the enrollment scores. In order to facilitate enrollment of large numbers of users, a medium level of fingerprint quality was considered acceptable. If, in practice, users enrolled at that level experience repeated biometric verification problems, those users should be re-enrolled to obtain a higher quality of biometric reference template. Experience with other implementations has shown that the quality of the reference template is a key predictor for successful verification in an operational setting.

LESSON: *Enrollment logs combined with active monitoring could identify persons where the reference template quality could improve their likeliness of success.*

5.7 Throughput Time Acceptance

Requiring the biometric validation to the entry process, added to the amount of time it took for a user to gain access to their spaces. The existing Prox system granted access to the user within a time frame of 1 to 2 seconds. The time to place the finger on the reader, obtain a live scan and do the comparison doubled the time to 3 to 4 seconds. While this was noted on several of the user surveys as an inconvenience, it was noted that this was an acceptable response time to obtain a higher security threshold.

LESSON: *Any modification to enhance security that increases throughput time needs to be balanced with the end-user's requirements to perform their duties and the volume of individuals gaining access at peak times.*

6. Future Opportunities and Next Steps

The CAC-PAC Norfolk Pilot fulfilled the expectations of both the eBusiness Office and SSC Norfolk by attaining established project goals and providing data on the use of contactless biometric equipment to enhance physical security in an operational setting. Additionally, data provided during the post-pilot evaluation will allow decision-makers to determine appropriate operational implementation issues with respect to future expansion of these capabilities at SSC Norfolk.

6.1 Necessary System Enhancements

This pilot clearly demonstrated the functional ability to utilize contactless biometric technology for controlling access to secured spaces. Additionally, it demonstrated the relative ease with which such technology may be integrated with an existing enterprise security infrastructure, especially when there is already an Electronic Security System (ESS) in place at those spaces. SSC Norfolk does not require any system enhancements at this time. They have a fully functioning system without any bugs. However, one enhancement that would provide additional benefit to the administrators would be a function to modify the requirement for biometric verification as threat conditions change. SSC Norfolk will need maintain an acceptable level of inventory of card stock for the enrollment of new users, and for the replacement of lost or damaged contactless cards.

6.2 Action Plan for SSC Norfolk

The CAC-PAC pilot remains in use for controlling access to the computer rooms at SSC Norfolk. Management has expressed the desire to continue to use the system in their operational environment. In addition, they would like to add biometric access for controlling access to warehouse areas and the SIPRNET room. The following steps are presented as a high-level action plan to accomplish this migration.

1. Identify the security requirements: the reason for enhanced security, prioritize spaces for the additional requirements, and obtain funding for the installation.
2. Order and maintain sufficient inventories of contactless card stock for use in the enrollment of new users, and for the replacement of lost and damaged contactless cards.

6.3 Enterprise Opportunity

This pilot demonstrated that biometrics on a Mifare embedded chip could meet the functional demands of the physical security community for door access control. However the next step may be caught in a circular loop: if the CAC is to fulfill its role as the physical security token for DoD, then it needs to incorporate the accepted technologies the ESS and physical security community uses for authentication. Likewise, if the physical security community wants to use the CAC as the physical security token, then it needs to clearly articulate what standards should be incorporated on the next-generation CAC. There is an enormous potential to reduce the number of physical security tokens used within DoD, but the cycle of requirements versus infrastructure must be resolved.

6.4 Enterprise Action Plan

In order to resolve the cycle of current CAC architecture versus requirements for next-generation CAC, an action plan has been generated to inform the correct individuals on the results of this pilot, gather concurrence regarding requirements, properly evaluate all potential solution, and facilitate a decision.

6.4.1 Short-Term Actions

DON eBusiness Operations Office has taken for action:

1. Provide pilot results to DON CIO, CNO N34 and DoD ACO
2. Continue to provide guidance to other Navy and Marine Corps organizations in regards to using the CAC as a physical security token by informing them of existing policies, current technologies trends and potential solutions to meet their specific needs.

6.4.2 Long-Term Actions

To fully develop the end state solution, several organizations across the services must agree on a CAC configuration that supports the requirements of the physical security community.

1. CNO N34, DON eBUSOPSOFF and DON CIO determine recommended DON platform.
2. CNO N34 presents architecture requirements to SEIWG.
3. SEIWG makes recommendation to SCSCG regarding technology requirements for physical security community.
4. SCSCG presents the DoD ACO with a configuration change request.
5. NSA to fully evaluate contactless security vulnerabilities, such as interception of contactless signals and key hacking.
6. Evaluate other technology solutions that meet the same function requirements.
7. DoD ACO to make contactless technology decision on the next-generation CAC.
8. SCSCG to determine space configuration on contactless chips, if necessary.
9. Define policies and deployment strategies that will encourage a transition to the next-generation CAC, as the DoD physical security token.
10. Define Issuance Strategy for next-generation CAC.

Appendix A Detailed Users Survey Results

SSC Charleston provided this appendix as part of their final report.

A.1 Overall Satisfaction

Overall satisfaction of the users of the technology was measured by analyzing the responses to the post-pilot survey question "What is your overall opinion of the pilot?" The possible responses to the question were:

0 – No Response Provided
1 – Disapprove
2 – Somewhat Disapprove
3 – Undecided
4 – Approve
5 – Absolutely Approve

There were 77 survey responses by users on the post-pilot survey. The breakdown of the answers to this question are shown here:

Pilot Opinion	**0**	**1**	**2**	**3**	**4**	**5**
Responses	*4*	*8*	*6*	*14*	*24*	*21*

The arithmetic average (mean) response for this item was 3.4, which places it between "Undecided" and "Approve". By discarding the non-responsive entries (i.e., those with the value "0"), the average (mean) rises to 3.6. For survey questions which have discrete numerical values, other measures of central tendency are probably a better descriptor of user opinion than the mean. The median value, which is the value which half of response lie above and half of response lie below, is "4", or "Approve". The mode, which is the most frequently occurring value, is also "4" or "Approve". The reasonable conclusion, based upon this analysis, is that the user opinions of the pilot were, in general, that they approved of the technology. Based on the initial goal of achieving a "4" on this survey question, the quantitative analysis supports the achievement of that goal.

A frequency histogram of these results is provided in the following figure:

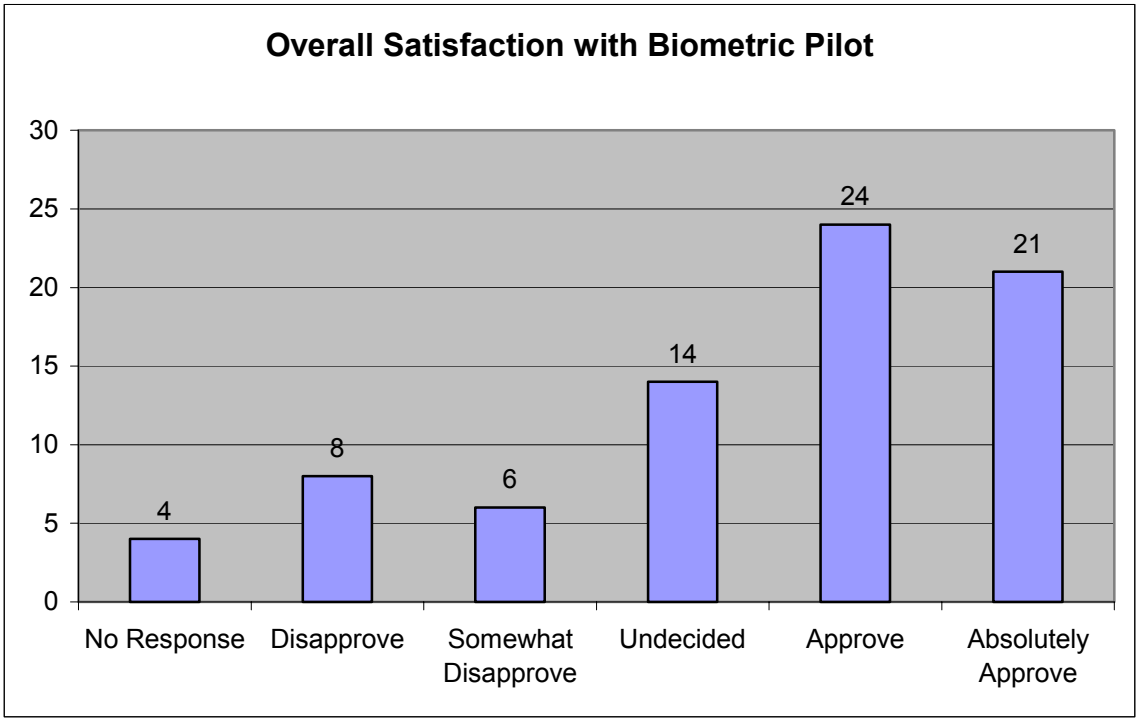

Figure 11: Overall Satisfaction

A.2 Increased Biometric Knowledge

Increased biometric knowledge among users of the pilot technology was measured by comparing the pre-pilot and post-pilot survey responses of users to the question "How familiar are you with biometric technology?". The possible responses to the question were:

0 – No Response Provided
1 – Not Familiar
2 – Somewhat Not Familiar
3 – Unknown
4 – Somewhat Familiar
5 – Very Familiar

There were 132 responses for the pre-pilot survey, and 77 responses for the post-pilot survey. The responses are shown in the following table:

User Familiarity	**0**	**1**	**2**	**3**	**4**	**5**
Pre-pilot	*0*	*71*	*21*	*26*	*8*	*6*
Post-pilot	*2*	*12*	*17*	*29*	*9*	*8*

The arithmetic means of the responses to this question were 1.9 for the pre-pilot survey, 2.7 for the post-pilot survey. This corresponds to an increase in user familiarity with the pilot

technology of approximately 42%. This exceeds the predetermined goal of a 25% increase in familiarity. The other measures of central tendency also reflect this strong increase in familiarity among the users after the completion of the pilot. The median value increased from "1" to "3", and the mode also increased from "1" to "3". This strongly indicates the success of the pilot in achieving the desired goal of at least a 25% increase in user familiarity with biometrics.

A frequency histogram of these results, normalized to percentage of responses to allow for the differing number of pre-pilot and post-pilot surveys returned, is provided in the following figure:

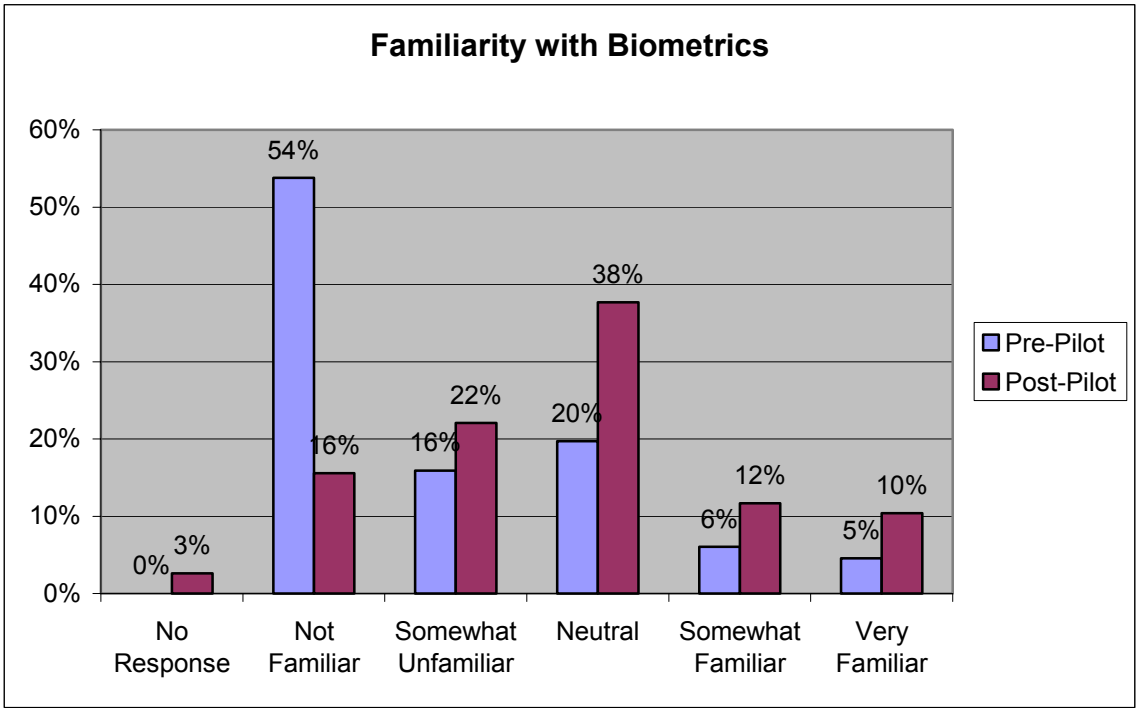

Figure 12: Familiarity with Biometrics

A.3 Increased feeling of security

Increased feeling of security among users participating in the pilot was measured by comparing the pre-pilot and post-pilot survey responses of users to the question "How secure do you feel in your spaces?". The possible responses were:

0 – No Response Provided
- 1 – Not secure at all
- 2 – Somewhat not secure
- 3 – Undecided
- 4 – Somewhat secure
- 5 – Extremely secure

There were 132 responses for the pre-pilot survey, and 77 responses for the post-pilot survey. The responses are shown in the following table:

How Secure?	0	1	2	3	4	5
Pre-pilot	*1*	*11*	*19*	*46*	*30*	*25*
Post-pilot	*3*	*4*	*11*	*25*	*21*	*13*

The arithmetic means of the responses to this question were 3.3 for the pre-pilot survey, and 3.3 for the post-pilot survey. By discarding the non-responsive entries (i.e., those with the value "0"), the means were 3.3 for the pre-pilot survey and 3.4 for the post-pilot survey. These results show only a very small positive change in the perceived level of security at the pilot site based upon the use of biometric technology. The other measures of central tendency showed similar results. The median and mode values, for both pre- and post-pilot surveys, were "3".

By normalizing the data to allow for the differing number of responses received for the pre-pilot and post-pilot surveys, and viewing the responses as percentage of respondents selecting each category, there is a small increase (from 42% to 44%) in respondents who felt "somewhat secure" or "extremely secure" in their spaces. This is a somewhat surprising result. It was anticipated that the use of biometric technology to verify identity prior to granting access would lead to an increased feeling of security among users in the controlled spaces. Perhaps what this indicates is merely that the users already felt generally secure in their controlled spaces, as one might anticipate in a military facility that utilizes electronic security systems for controlling access to physical spaces.

A frequency histogram of these results, normalized to percentage of responses to allow for the differing number of pre-pilot and post-pilot surveys returned, is provided in the following figure:

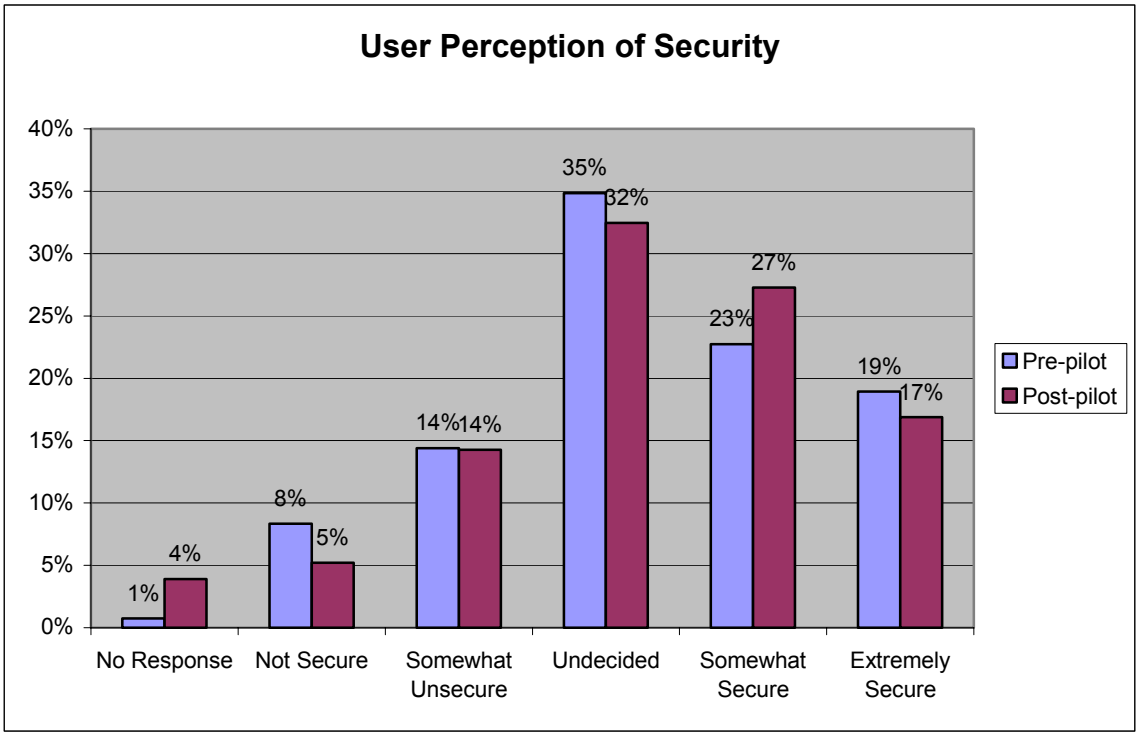

Figure 13: User Perception of Security

A.4 Ease of Access

Increased ease of access to facilities among users participating in the pilot was measured by comparing the pre-pilot and post-pilot survey responses of users to the question "How easy is it for you to gain access to the entry doors?". The possible responses were:

0 – No Response Provided
1 – No problems
2 – No problems reportable
3 – Had some problems
4 – Interference to my work
5 – Unacceptable problems

There were 132 responses for the pre-pilot survey, and 77 responses for the post-pilot survey. The responses are shown in the following table:

How Easy?	**0**	**1**	**2**	**3**	**4**	**5**
Pre-pilot	*2*	*109*	*17*	*4*	*0*	*0*
Post-pilot	*2*	*31*	*10*	*29*	*3*	*2*

The arithmetic means of the responses to this question were 1.2 for the pre-pilot survey, and 2.1 for the post-pilot survey. By discarding the non-responsive entries (i.e., those with the value "0"), the means were 1.2 for the pre-pilot survey and 2.1 for the post-pilot survey. These results show 76% and 78% decrease in perceived ease of use, respectively, by pilot participants. The other measures of central tendency are generally supportive of these values. The median increased from "1" to "2", but the mode was "1" for both pre- and post-pilot surveys. However, the second most commonly occurring value was "2" in the pre-pilot survey, and "3" in the post-pilot survey. All of these support the conclusion that the users found it more difficult to gain access to the entry doors after the implementation of the biometric technology.

A frequency histogram of these results, normalized to percentage of responses to allow for the differing number of pre-pilot and post-pilot surveys returned, is provided in the following figure:

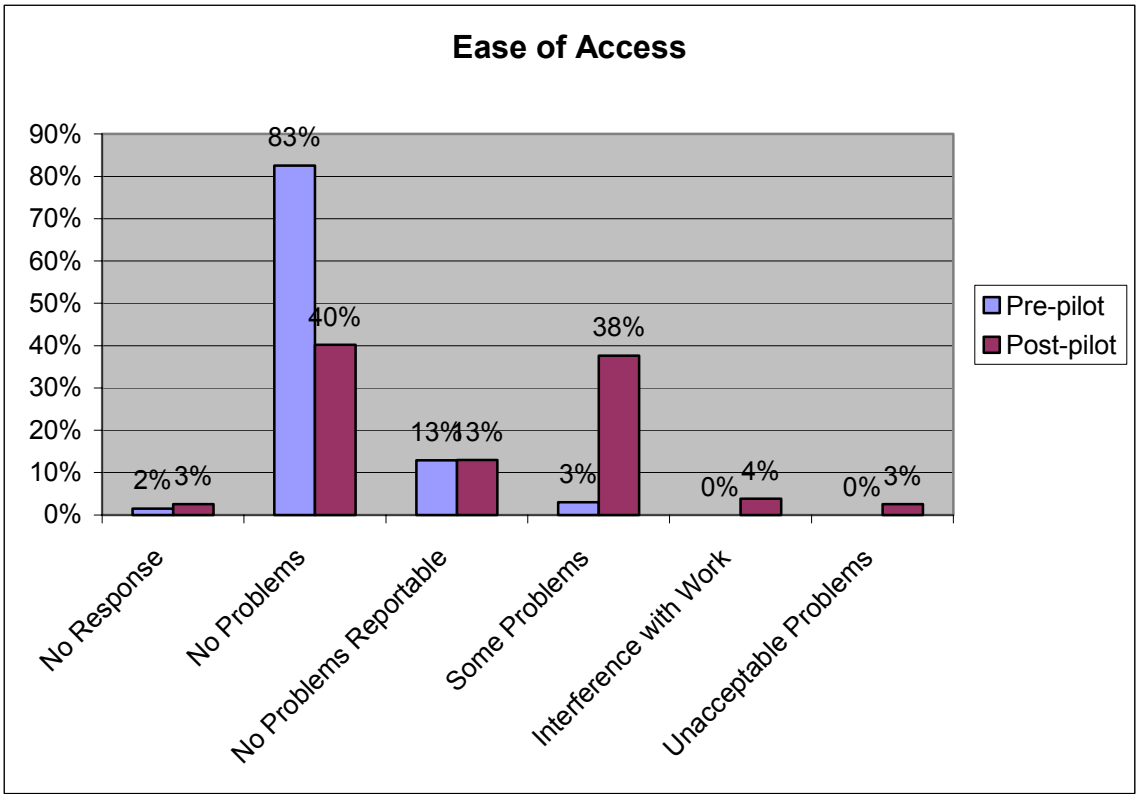

Figure 14: Ease of Access

This is not a surprising result. The pre-pilot access to the entry doors required only the use of a physical token; the biometric pilot required a token, in the form of a contactless smart card, as well as the subsequent presentation of a finger for biometric verification of identity. This is obviously more cumbersome, and the values reported by the users indicate that the users, in general, found it more difficult to gain access to the secured spaces through the use of biometric technology. While this was an expected result, the degree of decreased ease of use is a bit surprising. This may be the result of the ongoing problems experienced at Door 5 of Room A. These problems will be discussed at length in another section of this document.

A.5 Perception of Invasiveness of Technology

User perceptions of the degree to which biometric technology was viewed as an invasion of privacy was measured by comparing the pre-pilot and post-pilot survey responses of users to the question “Do you feel that biometrics are an invasion of your privacy?”. The possible responses were:

0 – No Response Provided
1 – Not Invasive
2 – Somewhat Not Invasive
3 – Neutral
4 – Somewhat Invasive
5 – Very Invasive

There were 132 responses for the pre-pilot survey, and 77 responses for the post-pilot survey. The responses are shown in the following table:

How Invasive?	0	1	2	3	4	5
Pre-pilot	*11*	*49*	*32*	*34*	*5*	*1*
Post-pilot	*2*	*44*	*14*	*11*	*4*	*2*

The arithmetic means of the responses to this question were 1.8 for the pre-pilot survey, and 1.7 for the post-pilot survey. By discarding the non-responsive entries (i.e., those with the value "0"), the means were 2.0 for the pre-pilot survey and 1.8 for the post-pilot survey. These results show a 12% decrease in the user perception of invasiveness upon completion of the pilot.

A frequency histogram of these results, normalized to percentage of responses to allow for the differing number of pre-pilot and post-pilot surveys returned, is provided in the following figure:

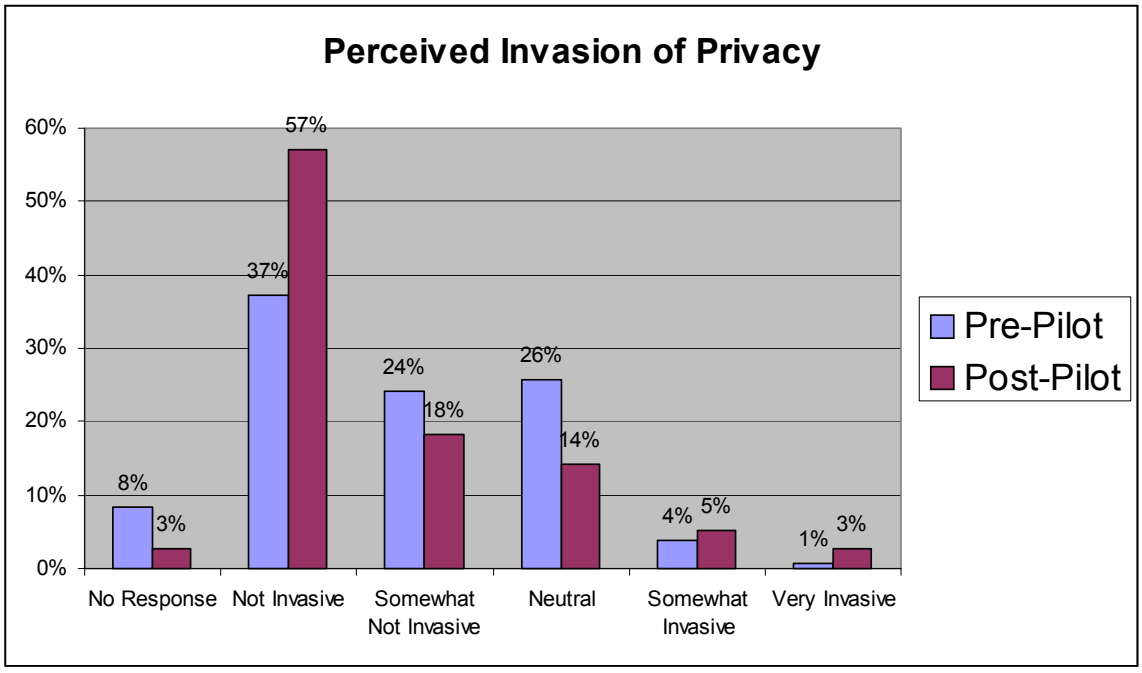

Figure 15: Perception of Invasion of Privacy

This is exactly the type of result one would hope for: that, after using a biometric system, the users understand that it is not invasive of their privacy, since the biometric is only being used for access control purposes, and not for any type of forensic purpose.

A second and related question asked of the users was “Do you feel the added security that biometrics provide offset any privacy concerns?”. The possible responses were:

0 – No Response Provided
1 – Disagree Strongly
2 – Disagree
3 – Neutral
4 – Agree
5 – Agree Strongly

There were 132 responses for the pre-pilot survey, and 77 responses for the post-pilot survey. The responses are shown in the following table:

How Invasive?	**0**	**1**	**2**	**3**	**4**	**5**
Pre-pilot	*11*	*26*	*16*	*45*	*11*	*23*
Post-pilot	*4*	*20*	*14*	*20*	*10*	*9*

The arithmetic means of the responses to this question were 2.7 for the pre-pilot survey, and 2.5 for the post-pilot survey. By discarding the non-responsive entries (i.e., those with the value “0”), the means were 2.9 for the pre-pilot survey and 2.6 for the post-pilot survey. These results show a 9% decrease in the user perception that improved security offsets any concerns about privacy upon completion of the pilot.

A frequency histogram of these results, normalized to percentage of responses to allow for the differing number of pre-pilot and post-pilot surveys returned, is provided in the following figure:

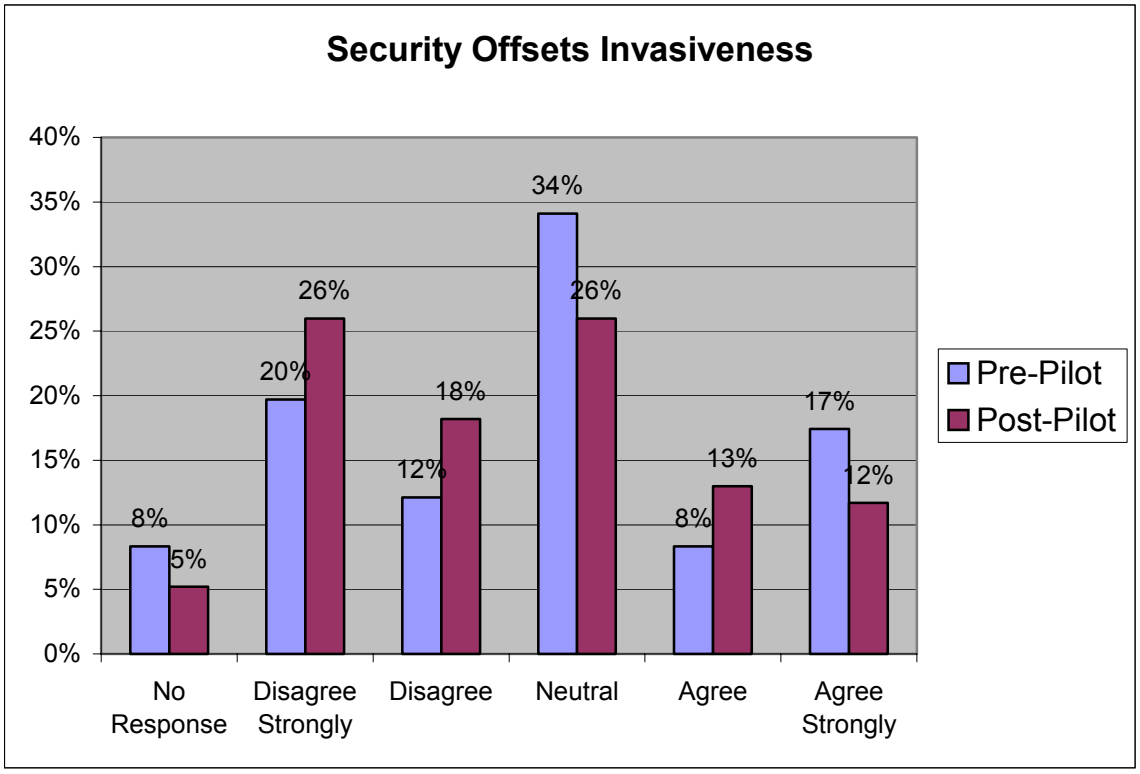

Figure 16: Security Offets Invasionness of Biometrics

These results are a little surprising, in light of the answers to the preceding question. Since the user perception of the invasiveness of the biometric technology went down as a consequence of the pilot, it seems contradictory that the user perception that increased security offset those privacy concerns did not go down in a similar manner. It appears that, even though the users seem less concerned about privacy issues, they do not necessarily believe that increased security is more important to them than any potential invasion of their privacy.

Appendix B System Statistics

SSC Charleston provided this appendix as part of their final report.

B.1 Invalid Badge Rate

The invalid badge rate is the number of errors observed in the ESS logs which indicate an Invalid Badge, divided by the total number of instances where access was granted. Several Perl programs were written to parse the logs, examining the contents of the message fields and the date and time stamps of entries in those logs. These programs provided the summary statistics on accesses which were granted, as well as those which were denied. When one or more failed access attempts were followed in close temporal proximity by an "Access Granted" message, the failed attempts were assumed to be by the same user who ultimately was granted access. This allowed a determination of the number of attempts required before an access was granted, and the summary statistics were analyzed using that assumption.

There were also instances where invalid attempts were not followed by successfully attempts within a reasonable time span. These probably constitute cases in which a user abandoned efforts to get in and walked away from the system, or requested another user let them enter the controlled space. Unfortunately, the design of the messages passed from the Bioscrypt fingerprint readers to the Lenel ESS did not allow a determination of the identity of individuals who were not granted access. This was a significant shortcoming in the implementation of the pilot, and made it difficult to identify users who had repeated problems accessing the system. Discussions are under way with the vendors involved to avoid this problem in any future biometric pilots.

Upon examining the summary statistics, it was decided that the results could be grouped in the following manner:

- User granted access with no preceding failures
- User granted access with one preceding failure
- User granted access with two preceding failures;
- User granted access with three or more preceding failures.

The results of that analysis can be seen in the following table:

Number of Preceding Failed Attempts	0	1	2	3 or more
Door 5	48%	12%	12%	28%
Door 6	89%	9%	2%	0%
Door 13	92%	7%	1%	0%
Door 15	90%	7%	1%	1%
Door 21	87%	10%	2%	1%
Door 22	89%	9%	2%	0%

Figure 17: Access Rates by Door

A frequency histogram of these results is provided in the following figure:

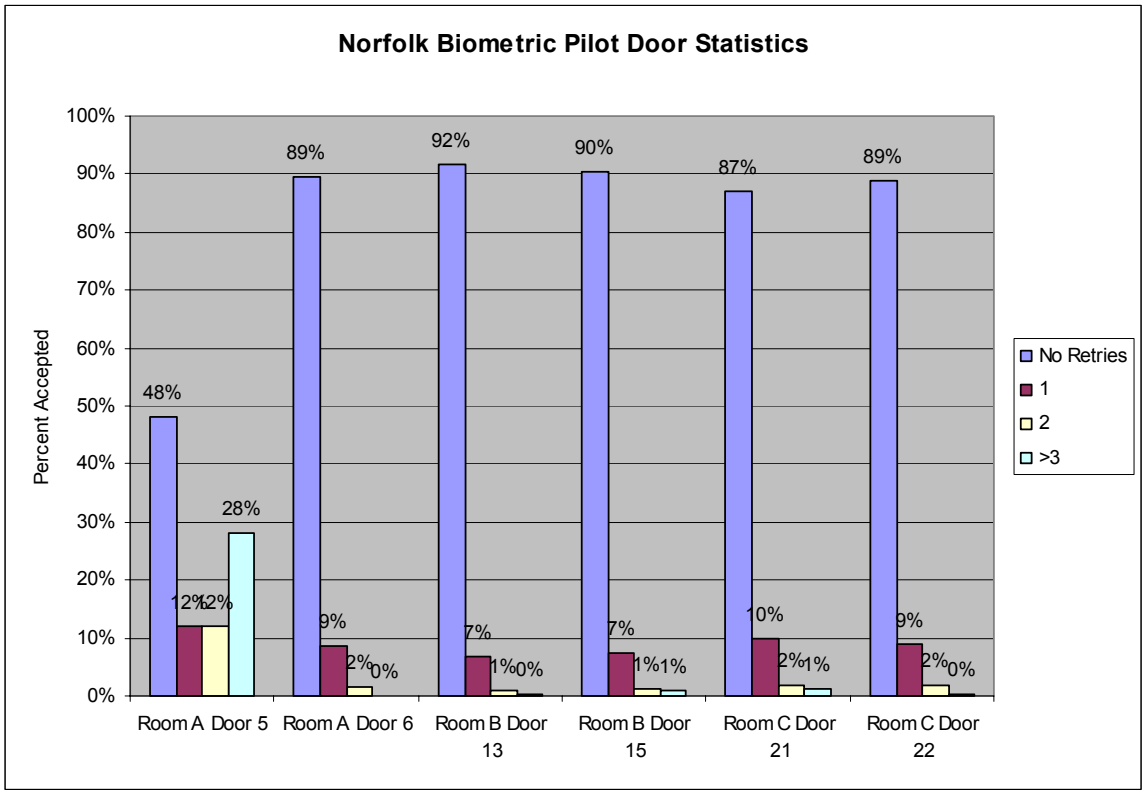

Figure 18: Door Access Statistics

With the exception of Door 5, Room A, the rates of access granted on the first try were in the general vicinity of 90%. This is consistent with the stated objective for this metric, which specified an invalid badge rate of 10% or less. If we define our conditions a little more generously, to allow for first time misplacement errors by users, the numbers are even more impressive. By defining our success as access granted with no more than a single retry, we obtain the following figures:

Door	Entry granted with one or less retries.
Door 5	60%
Door 6	98%
Door 13	99%
Door 15	98%
Door 21	97%
Door 22	98%

Figure 19: Entry Rates, One or Zero Retries

A frequency histogram of these results is provided in the following figure:

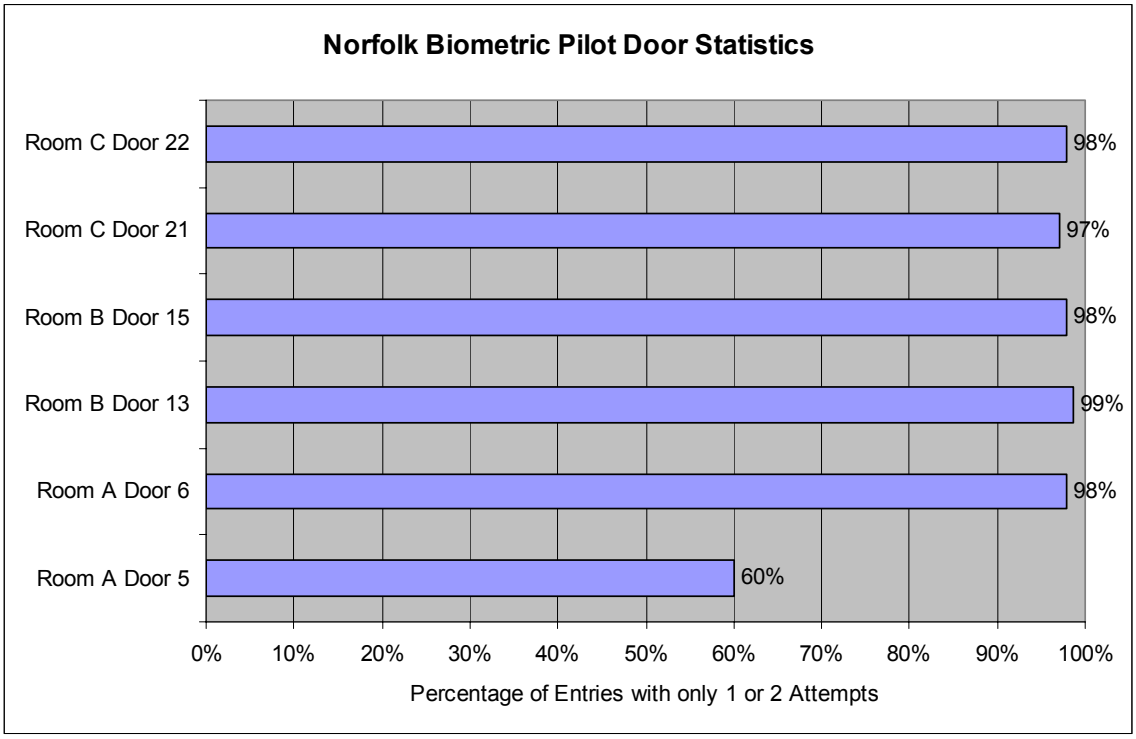

Figure 20: Door Entry Rates, 2 or Fewer Attempts

B.2 Decrease in Errors

The decrease in errors is a longitudinal measurement of error rates across time. It is typical, in a biometric pilot of this type, for error rates to be moderately high at the beginning of the pilot, but to decrease with time as users become acclimated to the use of the system. A Perl program was written to count all access granted messages and all invalid access messages in the Lenel ESS error logs. These values were grouped chronologically by date, and the average error rates for each of the three months in which the pilot occurred were calculated. The results of this analysis are shown in the following table:

Month	Observed Error Rate
August	*17.67%*
September	*12.50%*
October	*11.55%*

Figure 21: Monthly Error Rates

From August to September, the observed error rate decreased by 29%. From September to October, the observed error rate decreased by a further 8%. These were not as significant a reduction as had been set as a goal. The goal was a 50% reduction in the first month, followed by a further 25% reduction in the second month. The probable reason for these higher than anticipated error rates is the excessive errors experienced at Door 5. The details of this will be discussed at length elsewhere in this document.

A frequency histogram of these observed error rates is provided in the following figure:

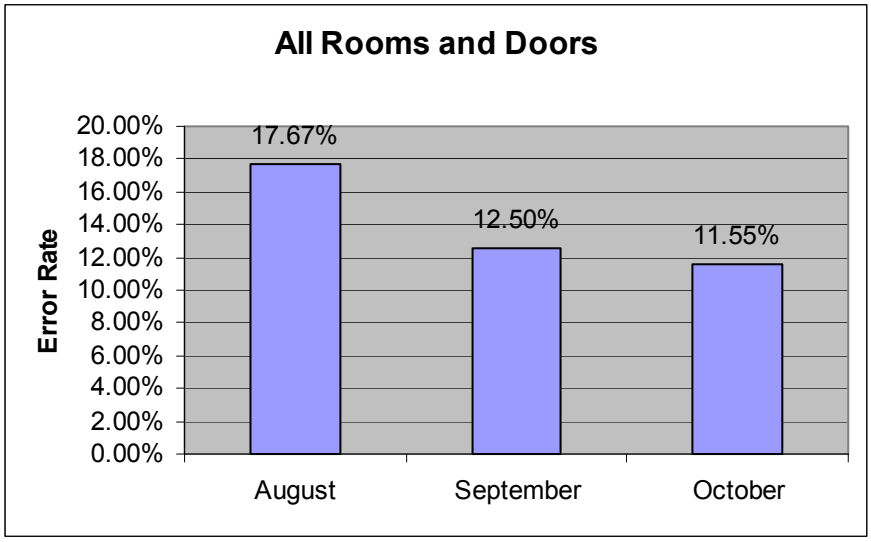

Figure 22: Error Rates by Month

While the general trend is as expected (decreasing in successive months), the magnitude of the trend is only half as great as had been set as the goal. An analysis of the raw data, excluding the data for Door 5, was attempted, in order to see if the excessive error rates observed at Door 5 were influencing the results disproportionately. By examining all the doors except Door 5, which had excessive error rates, the numbers were expected to be a bit closer to the predetermined goal for this metric. However, the results of that analysis did not bear out that expectation. The results of that analysis can be seen in the following table:

Month	Observed Error Rate
August	*16.34%*
September	*11.94%*
October	*11.22%*

Figure 23: Monthly Error Rates (Excluding Door 5)

This shows a decrease in error rate of 27% from August to September, followed by a further decrease of 6% from September to October. A frequency histogram of these results is provided in the following figure:

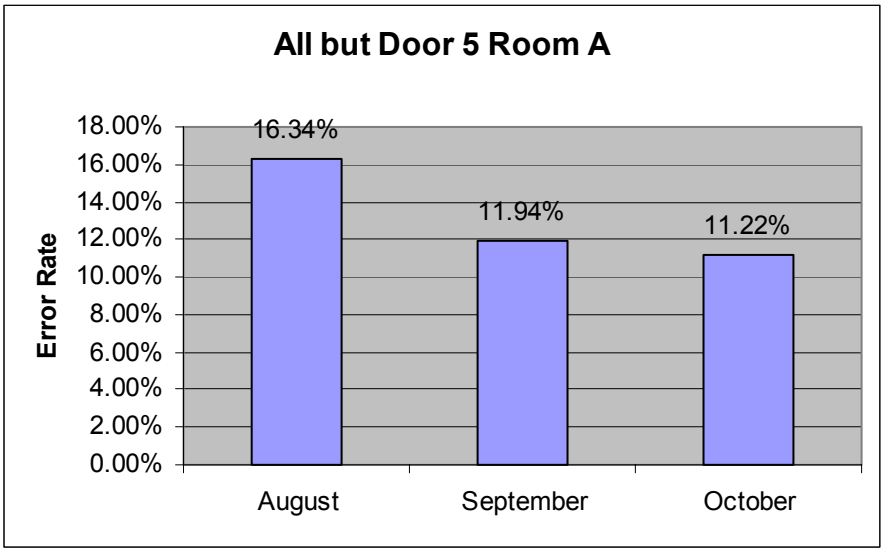

Figure 24: Error Rates by Month (Excluding Door 5)

The somewhat surprising conclusion is that Door 5 did not unduly influence the results for this metric. It is probable that in future pilot implementations of this type, the goals will be set less aggressively for this particular metric, since the decline in error rates appears to be significant, but not of the magnitude expected prior to this pilot.

B.3 Enrollment

The performance of the system with respect to the process of enrollment may be measured in two areas: speed of enrollment, and accuracy. During the enrollment process, paper forms were used to log the time required to enroll each user, how many attempts were required before a satisfactory quality of enrollment prints was obtained, and any descriptions of error messages observed or problems encountered while enrolling the user. Each enrollment captured prints for two distinct fingers, to allow users to obtain access to the controlled spaces even if one finger were injured or otherwise unavailable.

In the “best case” enrollments, users were successfully enrolled in sixty seconds or less, and only a single attempt was required in order to obtain an acceptable enrollment.

“Worst case” enrollments are fairly uncommon, but are very informative, since they represent cases that may be true of some percentage of any general population. It is worth reviewing a couple of these “problem enrollments” anecdotally.

In one enrollment, it took 5 minutes and 8 attempts before obtaining sufficient quality prints. In the description field for this record, it says that “right index and middle fingers did not work; burned his hand as a child; had to use right index and left thumb”. There is a definite probability that some percentage of any pilot user population will have experienced some type of injury which reduces the quality of fingerprint available. It will be necessary that the administrators tasked with enrolling users be aware of this possibility, and have standard procedures for dealing with it, such as attempting to enroll alternate fingers.

In another difficult enrollment, it took 10 minutes and 15 attempts before enrollment was successful. In the description field, the enroller wrote that "prints of left hand were all very poor; set security setting to very low". In some percentage of the general population, there will be individuals whose fingerprints are of such poor quality that it is impossible to get acceptable reference templates at the default system settings. In this situation, the enroller may have to modify individual security settings, as was done for this user, to allow that user to be verified with a poor quality print. This solution should only be used when all other methods fail, and only on systems where security settings may be set on a per-user basis. It would be inadvisable to globally lower the acceptable security thresholds for a biometric system, since it would greatly increase the likelihood of a determined attacker gaining unauthorized access to the system.

No specific goal was set for this particular metric. However, based upon an examination of the raw statistics collected during enrollment, it seems that in future biometric pilots, target goals could be set for this metric. The recommendation for this metric would be to complete an enrollment of a user (two fingers) in an average of two minutes or less, with an average of two attempts or less.

B.4 Ease of Administration

The determination of how easy it is to administer a system is largely subjective, and is based upon surveys of administrators of the system (pre-pilot and post-pilot), as well as through the collection of anecdotal evidence throughout the course of the pilot.

On the post-pilot surveys, neither of the administrators had any reportable problems gaining entry to the secured spaces. They both rated the enrollment process as "Easy", although one administrator noted that using the biometric system took longer than the pre-pilot system. Both rated maintenance levels the same as the pre-pilot system, and both indicated approval or strong approval of the pilot effort.

When asked whether the command had effectively communicated the purpose of the pilot, the administrators answered "Yes" and "Absolutely Yes". Both administrators answered that they did not view biometrics as an invasion of their privacy, and both reported feeling "Secure" or "Extremely Secure" in their controlled spaces.

Appendix C References

Helpful references on Security Guidance; Technology Reports, Other Research efforts:

1. Infineon Technologies. Security and Chip IC's SLE66CL160S Short Product Information 05.00, July 1999.

2. Philips Semiconductors, MIFARE Identification products. http://www-us.semiconductors.philips.com/identification/products/mifare/ (2001).

3. Lenel On-Guard. http://www.lenel.com/onguard/access.htm

4. Bioscrypt V20 Biometric Smart Card Reader. http://www.bioscrypt.com/products/vsmart.shtml

5. Smart Card Alliance. *Contactless Technology for Secure Physical Access: Technology and Standards Choices* dated October 2002. www.smartcardalliance.org.

6. Smart Card Alliance, Smart *Cards and Biometrics White Paper*, May 2002.

7. NIST Inter-Agency Report 6887: Government Smart Card Interoperability Specification (v2.0). *Briefing for M1-Biometrics*, August 22, 2002.

8. NIST Inter-Agency Report 6887 Government Smart Card Interoperability Specification (v2.0*), Presentation for: INCITS, B10.1 1C Cards with contacts, and B10.5 Contactless IC Cards*, August 14, 2002.

Appendix D List of Acronyms

Acronym	Definition
ACO	Access Card Office
BMS	Balanced Magnetic Switch
CAC	Common Access Card
CIO	Chief Information Officer / Chief Information Office
CNO	Chief of Naval Operations
CONOPS	Concept of Operations
DoD	Department of Defense
DON	Department of Navy
eBUSOPSOFF	DON eBusiness Operations Office
ESS	Electronic Security System
FAR	False Acceptance Rate
FRR	False Rejection Rate
GB	Gigabyte
HID	Hughes Identification Devices originally, now HID Corporation
ID	Identification
ISO	International Standards Organization
Kb	Kilobyte
KHz	Kilo Hertz
MB	Megabyte
MHz	Mega Hertz
NSA	National Security Agency
OA	Opportunity Analysis
PAC	Physical Access Control
PC	Personal Computer
PIN	Personal Identification Number
RAM	Random Access Memory
REX/PIR	Request to Exist / Passive Infrared Detector
SA	System Administrator
SCSCG	Smart Card Senior Coordinating Group
SEIWG	Security Equipment Integration Working Group
SIPRNET	Secure Internet Protocol Network
SPAWAR	Space & Naval Warfare Systems Command
SSC	SPAWAR Systems Center